

March 2, 2011

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Ex Parte Presentation

WT Docket No. 06-150; PS Docket No. 06-229; GN Docket No. 09-51

Dear Ms. Dortch:

We are pleased to submit the attached study, “Public Safety Priority Access to Shared Commercial Networks” prepared by Roberson and Associates, LLC (“Roberson”) for inclusion in the above referenced proceedings.

Roberson and Associates, LLC prepared the study to evaluate how a commercial broadband wireless network, operating on a shared basis with a dedicated public safety network in the 700 MHz band, can meet public safety priority access requirements and provide transparent overflow capacity and enhanced geographic coverage when needed. The study demonstrates that commercial networks *can* guarantee initial access to public safety users under congested conditions; that they *can* provide a guaranteed level of capacity to public safety; and that commercial network priority access *can* be provided automatically without explicit public safety user action.

The study supports the conclusions of the National Broadband Plan that there are material benefits to a commercial 700 MHz network shared with public safety users. Those benefits include: faster and significantly cheaper build-out of the dedicated public safety network; higher overall network capacity for the dedicated public safety network; extended geographic coverage of the public safety network; and commercial economies of scale that provide public safety with early, economical access to user devices with leading-edge capabilities.

If there are any questions regarding the study, please contact the undersigned.

/s/ Thomas J. Sugrue

Thomas J. Sugrue
Vice President, Government Affairs
T-Mobile USA, Inc.
401 9th Street, N.W.
Suite 550
Washington, DC 20004

/s/ Lawrence R. Krevor

Lawrence R. Krevor
Vice President, Spectrum
Sprint Nextel Corporation
900 7th Street, NW
Suite 700
Washington, DC 2001



Roberson and Associates, LLC
Technology and Management Consultants

Public Safety Priority Access to Shared Commercial Networks

Prepared for Connect Public Safety Now by:

Roberson and Associates, LLC

Contributors:

S. Borkar
D. Roberson
K. Zdunek

Public Safety Priority Access to Shared Commercial Networks

Executive Summary

It is of the highest national priority to provide public safety agencies with a nationwide, interoperable, broadband wireless network in the 700 MHz frequency band. To that end, within the 24 MHz of spectrum at 700 MHz already granted to public safety by Congress, the FCC has allocated 10 MHz for a dedicated broadband public safety network. There has been vigorous public debate about the amount of spectrum that public safety requires for broadband wireless, and several alternatives exist to provide public safety with additional capacity.

The first, enacted into law, is to auction 10 MHz of spectrum immediately adjacent to the already dedicated public safety broadband spectrum (the D-Block) to commercial use, and provide incentive-based public-private partnerships to fund the deployment of a high-capacity broadband network that would provide interoperable, priority access to public safety users when the dedicated public safety network becomes congested.

The second alternative, requiring new legislation, is to re-allocate the D-Block to public safety, and construct a dedicated network using the combined D-Block and already dedicated public safety broadband spectrum.

Another alternative is to re-allocate the D-Block to public safety, with the requirement that public safety partner with a commercial entity to build out the network, and that the commercial partner share the network, with priority given to public safety. Regardless of the amount of spectrum made available to public safety on a dedicated basis, and regardless of which of three alternatives above is selected, there is the recognition that during extreme public safety incidents, there will always be the need to provide public safety additional capacity beyond that available in an isolated network.

This technical study adds a key element to the public debate by addressing the issue of how a commercial broadband wireless network, operating on a shared basis with a dedicated public safety network in the 700 MHz frequency band, can meet public safety priority access requirements and provide transparent overflow capacity and enhanced geographic coverage when needed. The study refutes the criticisms that commercial networks cannot guarantee initial access to public safety users under congested conditions; that they cannot provide a guaranteed level of capacity to public safety; and that commercial network priority access cannot be provided automatically without explicit public safety user action.

Key elements of the priority access method for public safety on a shared commercial network are:

- Use of the Long Term Evolution (LTE) standard by both the public safety and commercial networks.

- Use of new priority mechanisms inherent to the Long Term Evolution (LTE) standard. These mechanisms have not been available on any wireless networks to-date, and provide effective alternatives to the idea of “ruthless preemption” on legacy circuit-based networks.
- Sharing of Radio Access Network (RAN) elements between the commercial network and dedicated public safety network, coupled with a Network Service Agreement (NSA) between the commercial and public safety entities.
- The dedicated public safety and commercial networks have their own Long Term Evolution (LTE) and Evolved Packet Core (EPC) entities.
- Appropriate provisioning of the public safety and commercial user devices.

Key characteristics of the priority access method are:

- Public safety traffic is routed through the public safety LTE core. Public safety maintains control over its traffic, its users, and its chosen method of prioritization.
- Public safety devices utilize the dedicated public safety network first, if it is available.
- A network access method that prevents commercial users from blocking public safety users from connecting to the network during periods of high demand.
- Public safety users are automatically handed-over to the co-located commercial network when the public safety network is congested, and handed back when capacity is again available.
- Public safety user traffic is prioritized on the commercial networks as on the dedicated network.
- A guaranteed amount of capacity is available to public safety users on the commercial network.
- The guaranteed capacity amount can be increased or decreased by network management action if necessary.
- Commercial users have access to all the commercial network capacity, if it is not being used by public safety users.
- An LTE preemption process that allows public safety users to be assigned bandwidth on a busy traffic channel.

Key enablers to realizing commercial and public safety network sharing are a supportive regulatory structure that promotes competition between commercial providers to create shared networks and support of the inclusion of all LTE operating bands in all 700 MHz devices, including Band 14 on which dedicated public safety broadband spectrum equipment will work.

The sharing of commercial network bandwidth with dedicated public safety bandwidth according to the methods described in the study confers significant advantages to public safety. These include: faster and significantly cheaper build-out of the dedicated public safety network due to the sharing of radio network elements with the commercial provider; higher overall network capacity for the dedicated public safety network by leveraging a high cell-density, commercial radio access network build-out; extended geographic coverage due to the ability to utilize commercial networks wherever they exist; and commercial economies of scale that provide public safety with early, economical access to user devices with leading-edge capabilities.

Table of Contents

Executive Summary	2
1.0 Introduction.....	10
1.1 Study Scope and Context.....	12
2.0 Overall Public Safety Priority Management Requirements	13
2.1 Public Safety User Categories, Classes, Modes, and Applications.....	13
2.2 Provisioning Requirements.....	16
2.3 Initial Connectivity.....	17
2.4 Public Safety Access during Network Congestion and Hand Over.....	17
3.0 LTE/EPC Based Public Safety Solution.....	18
3.1 LTE/EPC Overview	18
3.2 LTE/EPC Priority Mechanisms	19
3.3 Application of LTE Priority Mechanisms to Public Safety Users.....	21
3.4 Public Safety and Commercial Users in a Common Network	25
4.0 Assumptions and Shared Network Context	28
5.0 Public Safety and Shared Commercial Network Solution.....	30
5.1 Representative Shared Network Architectures.....	31
5.2 Requirements for Public Safety and Shared Network Environment	33
5.2.1 General Requirements in Shared Environment.....	34
5.2.2 Hand Over at Cell Edges to another Public Safety Network.....	38
5.2.3 Hand Over due to Congestion into Shared Commercial Network.....	38
5.3 Implications on Public Safety and Shared Commercial Networks.....	41
5.3.1 General	41
5.3.2 Impact on Network Elements.....	46
5.3.2.1 Public Safety Network Elements.....	46
5.3.2.2 Commercial Network Elements.....	48
6.0 Public Safety Users in the Shared Network Environment.....	48
6.1 User Scenarios (Use Cases).....	48
6.2 New Public Safety User – Public Safety Network not Congested.....	50
6.3 New Public Safety User – Public Safety Network Congested, Commercial Network not Congested.....	50

6.4 Existing Public Safety User Requests Additional Resources – Public Safety Network Congested, Commercial Network not Congested	51
6.5 New Public Safety User – Public Safety Network Congested, Commercial Users Using Public Safety Capacity.....	51
6.6 New Public Safety User – Both the Public Safety and Shared Networks Congested.....	52
6.7 Public Safety User in Shared Network – Hand Back to Public Safety Network	52
6.8 Commercial User in Commercial Network.....	53
7.0 Rules of Engagement / Agreements between Public Safety and Commercial Organizations.....	54
8.0 Additional Support from LTE Standards for Handling Public Safety Priority Management	56
9.0 Other Illustrative Shared Network Architectures.....	57
9.1 Shared RAN Architecture.....	57
9.2 Independent Public Safety and Commercial Network Architecture	57
10.0 Applicability and Extensions of this Study.....	58
10.1 Extended Public Service and Federal Community.....	58
10.2 Other Network Connections for Public Safety Users.....	60
10.3 Handling of a Data (ftp) Application	62
10.4 Public Safety Private Data Network (PSPDN)	62
10.5 Allowing Commercial Users into the Public Safety Network	63
10.6 LTE/EPC Evolution	64
10.6.1 LTE Releases.....	64
10.6.2 IP Multimedia Service (IMS) and Multimedia Priority Service	65
10.7 Items for Further Discussion	65
11.0 Conclusion.....	66
References	69
Acronyms.....	73
Appendix A: LTE/EPC Overview and Priority Mechanisms	76
A.1 LTE/EPC Introduction	76
A.2 User Equipment (UE)	78
A.3 Connections, Session Establishments, and Hand Overs	79
A.4 LTE/EPC Priority Mechanisms.....	83
A.4.1 Access to Air Interface and Attach Activities	83
A.4.2 Dedicated Traffic Bearer on Request.....	85
A.4.3 Priority Treatment Activities	88

A.5 Related Functions.....	91
Appendix B: Shared Network Architectures.....	93
B.1 Both RANs Connected to Public Safety EPC Core.....	93
B.2 Shared RAN Architecture	94
B.3 Independent Public Safety and Commercial Networks.....	95
Appendix C: PS_eNodeB and PS_PCRF Activities Summaries.....	97
C.1: PS_eNodeB Activities.....	97
C.2 PS_PCRF priority Management.....	97
Appendix D: Public Safety User Scenarios.....	99
D.1 New Public Safety User – Public Safety Network not Congested	99
D.2 New Public Safety User – Public Safety Network Congested, Commercial Network not Congested.....	101
D.3 New Public Safety User – Both the Public Safety and Shared Networks Congested	102
D.4 Public Safety User in Shared Network – Hand Back to Public Safety Network.....	104
Appendix E: Alternative Shared Commercial Architectures.....	106
E.1 Shared RAN Architecture.....	106
E.2 Independent Public Safety and Commercial Network Architecture.....	111
Appendix F: Public Safety User Roaming.....	114
Appendix G: X2 Interface Based Data Application Hand Over (HO)	116
Appendix H: Company Profile.....	118

List of Figures

Figure 1.1: Dedicated Public Safety and Shared D-Block Commercial 700 MHz Spectrum.....	10
Figure 1.2: Applicability of Priority Access Study: 700 MHz Band Where LTE is Used.....	12
Figure 3.1: LTE/EPC Architecture [3GPP10, Fig. 4.2.1-1]	19
Figure 3.2: LTE/EPC Priority Management Mechanisms	20
Figure 3.3: LTE/SAE Bearers [3GPP16, Fig. 13.1-1].....	21
Figure 3.4: Representative User and Service Mapping Illustration.....	22
Figure 3.5: Public Safety Users not blocked under Congestion Situation	26
Figure 5.1: Both RANs Connected to Public Safety EPC.....	31
Figure 5.2: Shared RAN Architecture	32
Figure 5.3 Independent Public Safety and Commercial Networks	33
Figure 5.4: Public Safety User Equipment Operation	36
Figure 5.5: Public Safety Broadband Interoperability.....	40
Figure 5.6: Network Interoperability and Equipment Startup.....	41
Figure 5.7: A Representative Dedicated Public Safety and Shared Commercial Architecture	42
Figure 5.8: Commercial RAN Public Safety and Commercial Usage Scenarios.....	43
Figure 5.9: Available capacity for Public Safety and Commercial users in the Shared Commercial eNodeB	45
Figure 5.10: Priority treatment for Public Safety User	46
Figure 6.1: Public Safety User Handed Over to the Commercial RAN in case of Public Safety RAN Congestion.....	49
Figure 10.1: Commercial User Allowed in Public Safety RAN; Commercial traffic through C_EPC	64
Figure A.1: 700 MHz E-UTRA Operating Bands	78
Figure A.2: S1 Based Hand Over (HO).....	81
Figure A.3: X2 Based Hand Over (HO)	82
Figure A.4: Policy and Charging Control (PCC) Elements.....	88
Figure A.5: Bearer Establishment for a Public Safety and a Commercial User in a Non-Congested Situation.....	90
Figure A.6: Bearer Establishment for a Public Safety User in a Congested Network.....	91
Figure B.1: Separate Network Access Network	94
Figure B.2: Shared Radio Access Network.....	95
Figure B.3: Separate Radio Access Networks.....	96

Figure C.1: eNodeB Procedure Summary for Public Safety user Radio Admission and Initial Attach97

Figure C.2: Public Safety User Priority Treatment in the Public Safety Network for Overloads in Both Networks98

Figure D.1: New Public Safety User in an Unloaded Dedicated Public Safety Network (Summary)...99

Figure D.2: New PS User in an Unloaded Dedicated Public Safety Network (Key Steps)100

Figure D.3: Public Safety User Moving into the Shared Commercial RAN (Commercial RAN Not Congested).....101

Figure D.4: New Public Safety User in a Congested Public Safety Network – Priority Treatment....103

Figure D.5: Public Safety User in Shared Network – Hand Back to Public Safety Network.....104

Figure E.1: Available capacity for Public Safety and Commercial users107

Figure E.2: Capacity Data for MME Load Decision108

Figure E.3: Shared RAN Public Safety and Commercial Traffic Management.....109

Figure E.4: Load Management in Shared RAN – Preemption of Commercial User.....110

Figure E.5: Public Safety Users at Their Capacity Limit – Priority Treatment within Public Safety Community.....111

Figure E.6: Home Routed Scenario for Public Safety user in the Shared Commercial Network112

Figure E.7: Local Breakout Scenario for Public Safety User in the Shared Commercial Network.....113

Figure F.1: Public Safety User Roaming into a Visitor Public Safety Network (Local Breakout).....114

Figure F.2: Public Safety User roaming into a Visitor LTE Based Commercial Network (Home Directed).....115

Figure G.1: X2 Based Hand Over (HO)116

Figure G.2: User Data Traffic Continuity for UE.....117

List of Tables

Table 3.1: Radio Access Illustration.....	23
Table 3.2: Allocation and Retention Illustration	24
Table 3.3: Application Bearer Treatment Example.....	25
Table 3.4: Radio Access for Public Safety and Commercial Users in a Shared Network	26
Table 3.5: Allocation and Retention Approach for Mixed Users in a Shared Network.....	27
Table 3.6: Public Safety User Bearer Priority Treatment	28
Table 10.1: Public Safety and Other Public (OP) Persons – Radio Admission Control.....	59
Table 10.2: Public Safety and Other Public (OP) Persons – Allocation and Retention Priority (ARP)	60
Table 11.1: Public Safety User Priority with respect to Commercial Users	67
Table 11.2: Priority Access in Networks – Public Safety and commercial.....	68
Table A.1: UE Classes	78
Table A.2: Radio Access Priority (Suggested in 3GPP).....	84
Table A.3: QCI to Packet Priority Mapping	87
Table A.4: Priority Attributes Assignment Template.....	89

1.0 Introduction

In order to satisfy the critical communications requirements of first responders, there must be a nationwide, broadband interoperable public safety network [CALD]¹. In response, the Federal Communications Commission (FCC) has licensed 10 MHz of spectrum in the 700 MHz band for a dedicated public safety broadband network, in addition to 12 MHz of spectrum in the 700 MHz band that may be used for narrowband (typically voice) applications and the 2 MHz of spectrum used as an internal guard band between the public safety broadband and narrowband segments.

The National Broadband Plan (NBP) [FCC1] contemplates pairing the 700 MHz D-Block commercial spectrum with the public safety broadband spectrum in order to create a public/private network accessible by public safety entities when the capacity of the public safety network is insufficient to meet first responders' needs (see Figure 1.1). The NBP also encourages public safety roaming across the entire 700 MHz band. This is a major advantage to the public safety community because it provides competitive options to them. Even if the D-Block is the primary focus of an incentive based partnership, the public safety agencies can partner with any 700 MHz licensee.

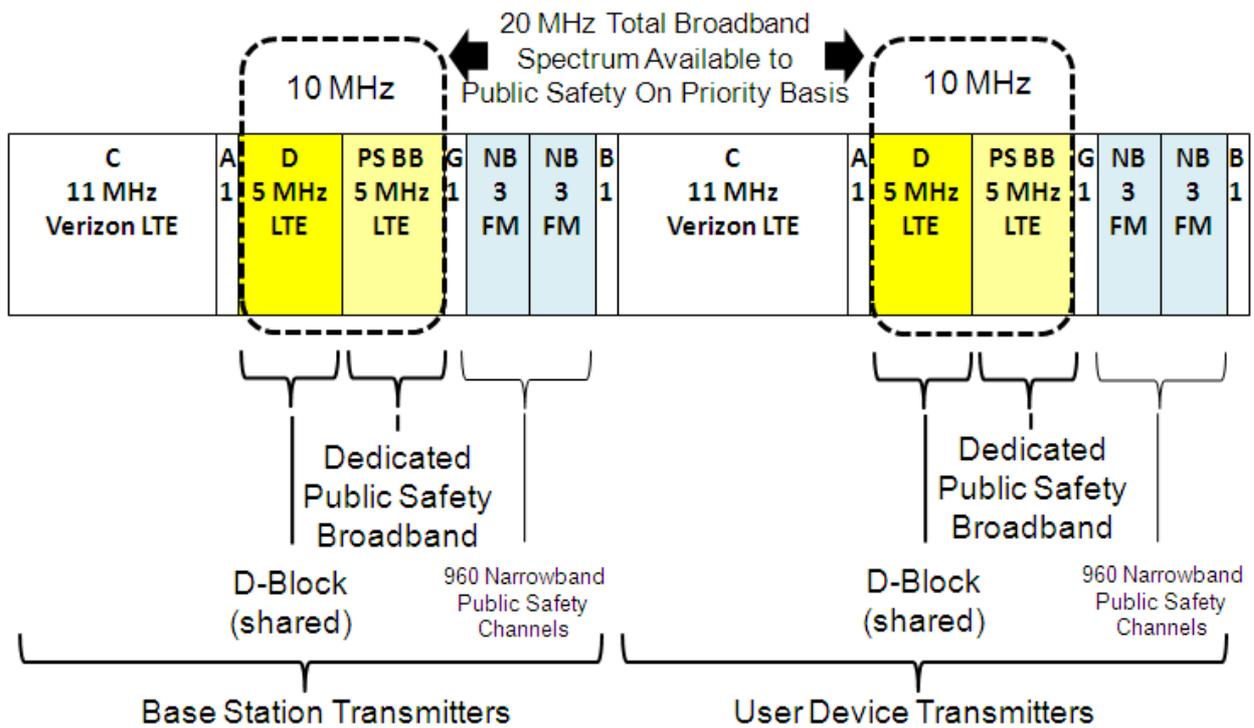


Figure 1.1: Dedicated Public Safety and Shared D-Block Commercial 700 MHz Spectrum

¹ References shown as [label] are grouped at the end of this document in order to preserve clarity.

This study demonstrates the feasibility and desirability of implementing an incentive-based public/private 700 MHz broadband network. The Long Term Evolution (LTE) / Evolved Packet Core (EPC) based architecture allows public safety officials, and not the operator of the commercial network, to control and prioritize their own communications traffic. A Network Service Agreement (NSA), negotiated between public safety and commercial entities, would specify how the prioritized public safety traffic would be carried on the commercial network.

The proposed architecture is robust and the LTE/EPC priority structure ensures that the priority requirements of public safety users are met when a public safety user moves into the shared commercial network. Specific mechanisms for priority access, in particular, LTE capabilities, are used in representative first responder scenarios to demonstrate priority access. The study is expected to provide a starting point for the development of a more complete architecture using a shared network.

Section 2 of the study highlights the public safety priority-related user needs as identified by key public safety entities and trade groups to establish a framework for first responder's priority access. An overview of the LTE/EPC architecture and the associated priority mechanisms are available in Section 3. The key assumptions for the shared network architecture are provided in Section 4. In order to apply the LTE/EPC priority mechanisms for the shared environment, three distinct architectural alternatives are proposed in Section 5. The section also closely examines how public safety traffic can be prioritized through the use of a dedicated and a shared commercial RAN and separate public safety and commercial EPCs. The network architecture is then applied to the requirements defined in Section 2. This is followed by a discussion of how public and commercial users are provisioned on the commercial network and how the public safety user Hand Over (HO) is automatically handled without public safety user or operator intervention.

Representative scenarios for initial connection and subsequent support of public safety traffic, especially for congestion situations, are covered in Section 6. The impact on commercial users due to the presence of public safety users in the shared commercial network is also highlighted. Section 7 provides the overall framework of the rules that the public safety and commercial licensee must observe in the shared network architecture. A Network Service Agreement (NSA) to establish these rules is also discussed.

The study shows that the LTE/EPC foundation, along with both a dedicated and a shared commercial network architecture, do provide robust priority treatment for the public safety users. Evolution of 3GPP technology could further enhance the public safety user experience. These recommendations are highlighted in Section 8.

In Section 9, the feasibility of the priority treatment for public safety users in the shared commercial architecture is demonstrated for two additional representative shared network architectures. Section 10 identifies the extensions and applicability of this study to other cases and situations including HO and roaming onto other LTE environments, data applications, and different approaches towards more optimum HOs.

Concluding remarks are followed by References, Glossary, and Appendices, The appendices provide additional technical details for the information in the main document.

1.1 Study Scope and Context

The primary intent of this study is to show that public safety priority requirements can be fully met when a public safety user moves (via HO) to a shared partner (D-Block or other 700 MHz) commercial network during public safety network congestion conditions. The shared architecture reinforces that the public safety agency managing the dedicated public safety network will maintain control of the public safety user priority management, especially during emergency situations.

There are also significant cost advantages that accrue to public safety via utilization of a shared approach. On the network side, the infrastructure cost to public safety is substantially reduced due to the co-location of base sites, towers, and radio network equipment. On the user device side, economies of scale driven by commercial volumes will result in lower device costs to public safety. The performance and cost aspects are described in detail in [ROBE], [OBI2], [FCC2]. The document and methods described are applicable wherever LTE technology is used. For convenience, however, this study primarily focuses on the D-Block and commercial network sharing in other parts of the 700 MHz band. See Figure 1.2 for an illustration of the 700 MHz band plan and the associated LTE opportunity blocks.

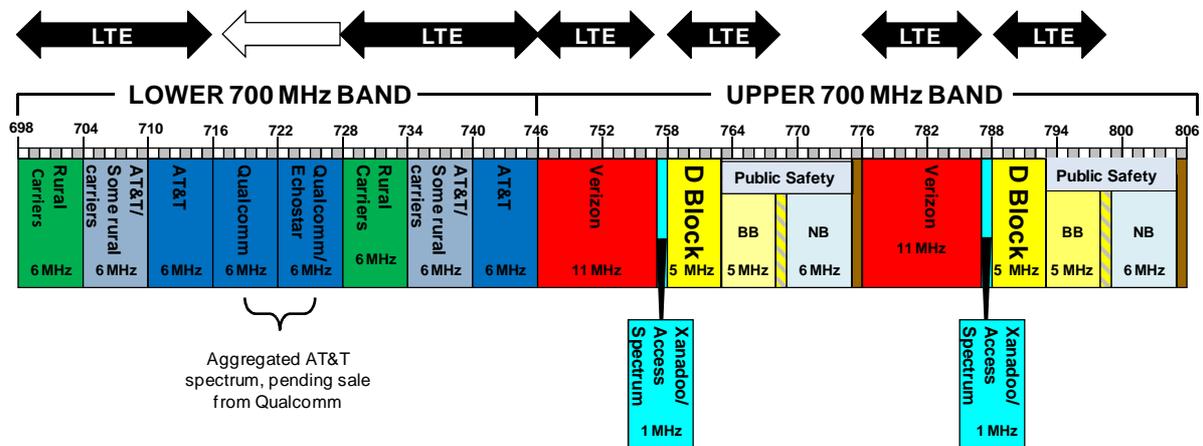


Figure 1.2: Applicability of Priority Access Study: 700 MHz Band Where LTE is Used

The focus is on requirements and scenarios as they pertain to priority management for public safety users. In a typical network, user's experience is dependent on network availability and network and customer management. Management involves monitoring and recovering from fault conditions, compiling billing records, and providing customer service. Topics such as network management and Operations Support System / Billing Support System (OSS/BSS) and operational and performance issues are considered to be beyond the scope of this study.

The study identifies the 3rd Generation Partnership Project (3GPP) LTE/EPC standards mechanisms for handling situations in which a public safety user moves from a dedicated public safety network to a shared commercial network. This is done by choosing a representative public safety and shared commercial architecture to illustrate the priority mechanisms and interfaces without precluding other architectures. The architecture in this study is not intended to constrain the design or implementation of a shared network, or provide a completely optimized solution. This study provides an example, demonstrating the feasibility and practicality for robust public safety priority treatment in a shared commercial environment. It is expected to be a starting point for a definitive approach for priority access for public safety on shared commercial networks.

The study is intended to be consistent with the current 3GPP standards (specifically the 3GPP Long Term Evolution (LTE) Release 8 standard – [3GPP16]) and the prevalent commercial operators' policies, deployments, and implementations wherever applicable. By following this approach, it is expected that the commercial platforms can be leveraged with minimal hardware modifications, and modest application level software, to accommodate public safety priority access requirements. For deployment of the shared network approach, the appropriate connections (interfaces) between the public safety core, commercial core, and public safety eNodeBs and commercial eNodeBs need to be provided, consistent with the sharing agreement that would be established between the commercial operator and public safety. Commercial and public safety user devices need to be provisioned in accordance with the methods described in this study. A video streaming application is used as a convenient example. The proposal for the definition of the capacity metric to be used for priority and scheduling purposes is provided in Section 4.0.

2.0 Overall Public Safety Priority Management Requirements

Using information from recognized public safety broadband requirements setting efforts [MILL], [NFPS], [NPST1], [NSEP], [PSST2], [OIT], this section summarizes the key requirements that public safety entities have enumerated regarding priority access. The requirements extracted here are intended to capture the essential public safety requirements independent of the network that the public safety user connects to, i.e., whether the network is a dedicated public safety network or a shared commercial network. The priority access approaches described in this study are sufficiently flexible that they can be adapted to accommodate future refinement of public safety broadband requirements that may occur. The approaches described here are also intended to be consistent with Next Generation Network / Government Emergency Telecommunications Service (NGN/GETS) [NSEP], wherever applicable.

2.1 Public Safety User Categories, Classes, Modes, and Applications

The network access and priority access mechanisms developed by public safety entities and described in this document apply to emergency response providers [NPST2] as described and categorized by the Homeland Security Act of 2002. These users include federal, state, and local entities engaged in emergency public safety law enforcement, emergency response, and emergency

medical services, including hospital emergency, and related personnel, agencies, and authorities. The specific focus is to support operational scenarios and first responders that include law enforcement, fire fighters, and emergency medical personnel. It is also the intention to include network use by “second-responders” that include agencies involved in disaster recovery and support functions.

In public safety communications, the concept of communication priority stems from the need to assign, in a pre-determined manner, the use of a limited-capacity wireless communication resource to the user or users with the highest level of need at any instant in time. For public safety, the mission-critical need at a specific point in time is determined by both 1) the position of the user in the public safety organizational hierarchy; and 2) the specific circumstance or situation in which the user is involved. For example, in order to communicate high-level command orders in a timely manner, it is essential that such orders have priority over less urgent (hierarchical) level communications. At times, however, the need for a user at a lower hierarchical level to communicate urgent information because of an immediate and serious life threatening situation must be met by elevating that user’s ability to use the communication channel, if temporarily. Based on these needs, the mechanisms for assigning communication priority for public safety on dedicated public safety networks must be met on networks that are shared with commercial users as well. Additional mechanisms to provide public safety users access and data throughput with a higher priority than commercial users must also be specified.

In traditional public safety narrowband voice communications networks, the wireless communication channel assignment and transmission mode are circuit-based, and typically, only one user equipment can transmit over a channel at any given time. In a broadband, packet-based data communications architecture such as one employing the LTE-based standard that will be used by public safety community in the 700 MHz band, data packets and packet streams from many users are multiplexed in time and frequency on the wireless medium. The result is that multiple users can be assigned simultaneous communication sessions. Prioritization on a packet network, and specifically on an LTE-based shared commercial network, will involve three levels and mechanisms within which priority principles will be invoked: 1) priority treatment for public safety network connection (access) requests; 2) priority treatment in the assignment of (packet) traffic bandwidth, with the ability to make room for priority packet streams on a congested network; 3) the instant-to-instant prioritization (scheduling) of packets for transmission. The assignment of traffic bandwidth for public safety includes reserving a pre-set, guaranteed level of capacity on the commercial network for public safety use.

A representative public safety hierarchical prioritization developed by public safety entities is indicated in the following, where 1 indicates the highest priority [PSCR2] [NSEP, Sec. 2.4.1]:

- Priority 1: Executive leadership and policy makers.
- Priority 2: Disaster response and military command and control.
- Priority 3: Public health, safety, and law enforcement command.
- Priority 4: Public services/utilities and public welfare.
- Priority 5: Disaster recovery (e.g. National Communications System).

The following additional requirements developed by public safety entities are also recognized:

- The network must provide 50% (or a minimum of 8) access priority levels based on the number of priority levels available in the radio access network technology. The public safety priority levels are to be the highest levels available, over and above those levels available to commercial users [NPST1].
- The network must allow for different levels of service to be defined based on the given hierarchical role of a public safety user [NPST1].
- The network and User Equipment (UE) must accommodate the following situational levels of priority (modes) for public safety users.
 - Normal Priority: Non-emergency mode, routine communications.
 - High-Priority: Emergency mode, incidental (exceptional) purpose communications.
- A public safety user in the high-priority, emergency mode, regardless of their hierarchical priority level, may be treated with higher priority than any other public safety user in a normal (non-emergency) mode. All public safety users, regardless of rank or organization, shall be permitted to use this level, typically through the use of a separate emergency button [NPST1].
- Mode of Operation Invocation.
 - The default will be normal mode. The public safety user will indicate the emergency mode of operation via an explicit indication, e.g., by pressing an emergency priority button. “Normal” priority modes for public safety are understood to be at a higher level than commercial priority levels.
 - If a non-public safety UE attempts to invoke public safety level priority, access will be denied and the incident along with the information about the user will be logged.
- A public safety user, regardless of their home location, may initiate a call / session anywhere in the country (nationwide access). However, public safety users in their home area shall have a higher priority than visiting public safety users [NPST1].

Public safety entities require the following representative services categories to be accommodated by the dedicated public safety and shared commercial networks include [NYC].

- Streaming real-time video, and file transfers including, but not limited to detailed maps and blueprints, and high-resolution photographs.
- Real-time video upload to the emergency operations center.
- High-definition video, high-resolution photos, and detailed maps to police vehicles.
 - Digital imaging, Global Positioning Information Systems (GPIS), Web access, Automatic Vehicle Location (AVL).

Public safety entities also identified the following representative application categories to be accommodated including seven required and four desired categories [NPST2]:

Required:

1. Internet Access.
2. Virtual Private Network (VPN) Access to any Authorized Site and to Home Networks.

3. Status / Information “Homepage”.
4. Status / Information “Short Message System (SMS)-Machine to Machine System (MMS) Messaging”.
5. Access to Responders under Incident Command System (ICS).
6. Land Mobile Radio (LMR) Gateway Devices.
7. Field-Based Server Applications (for a subset of users).

Desired:

1. Location Based Data Capability.
2. One-To-Many Communications across All Media.
3. Land Mobile Radio (LMR) Voice.
4. Public Switched Telephone Network (PSTN) Voice.

Since the primary intent of the broadband public safety network is understood to be the support of broadband *data* services, voice services will not be addressed further. It is expected that the priority mechanisms described here can be extended to voice, if desired.

2.2 Provisioning Requirements

Provisioning refers to the process by which new public safety UEs are given the ability to access the network via appropriate authorization settings, are given access to specific services, and are assigned network access and traffic priority levels.

Public safety entities identified the following provisioning capabilities as requirements for public safety users:

- The network shall provide the ability for the recognized public safety agency or authority to manage the public safety users on the network. Management means control, setup, and modification of user, user group, and application priority profiles. It includes the ability to provision, add, and authenticate users and user equipment.
- The Quality of Service (QoS) metrics and the priority levels for public safety users must be dynamically configurable by an appropriate authorized administrator [OIC].
- Mechanisms must be provided to enable networks to be provisioned to prioritize different types of service classes / packet streams for public safety users compared to commercial users.

As a key element of the ability of the public safety agency to manage public safety users on the shared network, public safety entities require that the communication usage statistics for public safety users must be collected, logged, and maintained.

2.3 Initial Connectivity

Based on the availability of a particular 700 MHz LTE network type in the geographic area in which the public safety UE finds itself, public safety entities require the UE to power up and initiate a communication session in a “Starting Network” according to the following priority:

- Dedicated, 700 MHz home public safety network.
- Dedicated, 700 MHz visited public safety network.
- Shared, 700 MHz (LTE based) commercial network.

2.4 Public Safety Access during Network Congestion and Hand Over

It is paramount that public safety users always be able to access and communicate on a network if it exists where the user is located, even if the network is operating at the limits of its capacity. Emergency communications capability as described above must always be provided. The following requirements are therefore necessary for public safety users on dedicated public safety networks, as well as networks shared with commercial operators (for example, D-Block networks):

- A public safety UE shall be able to successfully communicate with any available network with which the public safety agency has entered into a commercial partnership with. A public safety user should be able to initiate a data communication session, regardless of the loading level of the network. Control signaling for the purpose of establishing network access will not be blocked for public safety users.
- If a public safety user is using a public safety network that becomes congested, provision will be made such that:
 - The public safety user can move (be handed over) to an alternate network, if one is available. In any such HO situation, the continuity, performance, priority, security, and data integrity of the public safety user will be maintained.
 - The QoS of a lower priority user may be reduced, or a lower priority user may be preempted in order to free up resources for a higher priority user.
 - HO necessitated by network congestion is to be provided anywhere in the coverage area, including strong signal areas.
- Whenever a public safety user is in a weak signal area (e.g., at a cell boundary) and needs to be handed over to a new sector-cell, the public safety user’s session should continue in a transparent manner via HO to another sector-cell or network.

The requirement to reduce the service level of a lower priority commercial or public safety user (preemption) is not intended to conflict with the public safety requirements as described in [FCC3], which states that preemption of existing commercial calls is not to be allowed. The applicability of this requirement, developed in 2000 and before the capabilities of LTE were completely specified, is properly understood to be in the context of a voice service, not data services. Within a packet data architecture such as LTE, other alternatives are available to allow for new sessions on a busy

channel. These alternatives, which include packet scheduling on a very rapid basis, are discussed in subsequent sections of the document. It is also understood that data connections established with emergency priority will not be preempted.

3.0 LTE/EPC Based Public Safety Solution

The public safety community requires very robust and secure priority management of services end-to-end. Currently national security and emergency preparedness communications are given priority treatment by legacy GETS and Wireless Priority Service (WPS). These voice-based legacy services are provided by service providers' circuit-switched wireline and wireless networks. It is an imperative that the public safety's critical communications needs be met by the latest and most advanced packet transport and wireless access based technologies.

Previous studies have proposed the use of an LTE/EPC based solution to meet public safety community requirements [ALU1], [ALU2], [MOTO2]. The packet transport network can provide QoS-oriented treatment at a packet level and hence resources can be dynamically adjusted instant-by-instant depending upon the requirements of the application. Multiple applications can co-exist and be managed effectively. The Radio Access Network (RAN) provides high and flexible bandwidth as a foundation for a nationwide broadband network. Use of this industry standard technology should enable cost reductions based on economies of scale, leverage the vast experience of the commercial operators, and allow the public safety community to influence the standards bodies for advanced features needed by the its users. Also, substantial cost savings come from building networks based on the same technology, and partnering with commercial operators. It is expected that in the initial phases, the LTE/EPC based solution will support video and data applications. Voice connectivity will continue to be provided by existing LMR narrowband networks in the near future. Eventually, voice services will be provided on the LTE/EPC network, likely in the form of the IP Multimedia System (IMS)-based Voice over LTE (VoLTE) solution, appropriately adapted to meet public safety requirements.

3.1 LTE/EPC Overview

Appendix A provides an introduction to the LTE/EPC architecture and the associated priority schemes and mechanisms. These mechanisms can be applied to a dedicated public safety network as well as to shared networks where public safety and commercial users may co-exist. The overall architecture and the related entities as defined by the 3GPP standards are shown in Figure 3.1.

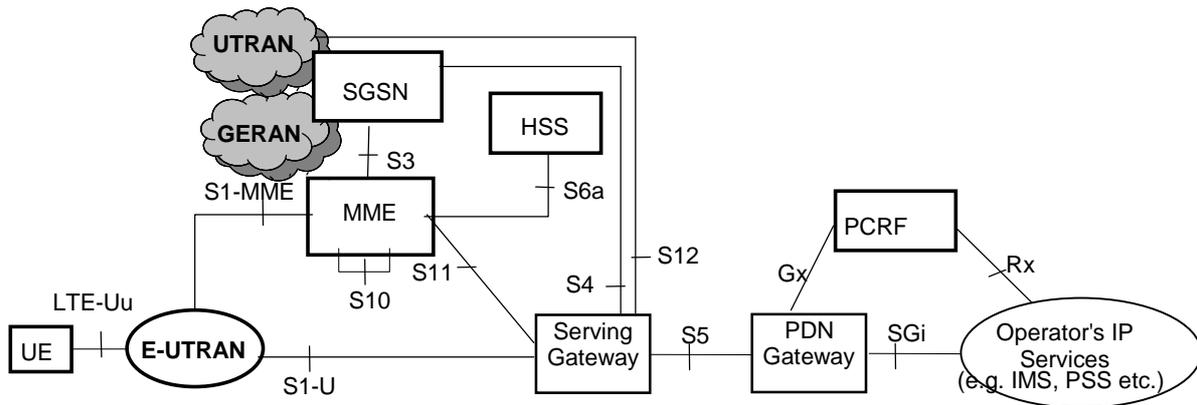


Figure 3.1: LTE/EPC Architecture [3GPP10, Fig. 4.2.1-1]

LTE/EPC is a comparatively “flat” Internet Protocol (IP)-based architecture with a RAN and a packet core [3GPP16], [MOTO3]. The RAN is an integrated base station / controller (eNodeB) complex called the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) [3GPP10, Sec. 4.2, Sec 4.4.1]. The core is designated as the Evolved Packet Core (EPC).

E-UTRAN is connected to EPC core via an S1 interface. The collection of eNodeBs can be interconnected with each other for signaling and packet forwarding purposes via the X2 interface.

The key elements in the EPC [ALU3] include the Mobility Management Entity (MME), Serving GateWay (S-GW), Packet Data Network (PDN) GateWay (P-GW), Policy and Charging Rules Function (PCRF), and Home Subscriber System (HSS) with a set of associated sub-systems. The MME [3GPP10, Sec. 4.4.2] provides the control plane functions related to subscriber and session management, equipment management and tracking, and location management [3GPP14, Sec. 5.2.1]. The S-GW [3GPP10, Sec. 4.4.3.2] provides packet data routing and is the user traffic mobility anchor. The P-GW [3GPP10, Sec. 4.4.3.3] is the default gateway to the PDN. It is responsible for packet filtering and QoS enforcement. The PCRF [3GPP8, Sec 6.2.1], [3GPP10, Sec. 4.4.7], [3GPP12, Sec. 4.4] is the centralized rules engine for priority management. The HSS stores and updates a database [3GPP10, Sec. 5.7.1] with user’s subscription information, International Mobile Subscriber Identity (IMSI), and approved QoS profiles. Additional details about these entities and the connections, session establishment, and HO operations can be found in Appendix A.

3.2 LTE/EPC Priority Mechanisms

The focus of this study is priority management for public safety users in a shared commercial network. In addition to the standard commercial features, public safety can utilize additional LTE features which may include cell barring for commercial users, cell reservation, special access classes, LTE user preemption, and LTE application preemption.

The application of the public safety priority support has been studied previously in several documents and studies [PSCR1], [PSCR2]. A good foundation for the understanding of public safety priority management is also provided in [HALL], [BROU], [PSCR2]. In particular, the joint National

Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) Public Safety Communications Research (PSCR) team in Boulder, CO has a working demonstration using multiple streaming video sessions with “Best Effort” priority schemes, and is exploring the application of the priority schemes for public safety users on dedicated public safety networks. This study builds upon and augments the comprehensive collaborative effort at NIST/NTIA.

Overall, the sequence of steps to set up an application for a public safety user can be grouped into two major steps (see Figure 3.2): 1) Radio access (access to the system, especially in times of congestion), initial radio connection, and attach (allocation of transmission channels); and 2) Establishment of an application oriented traffic bearer (packet priority allocation).

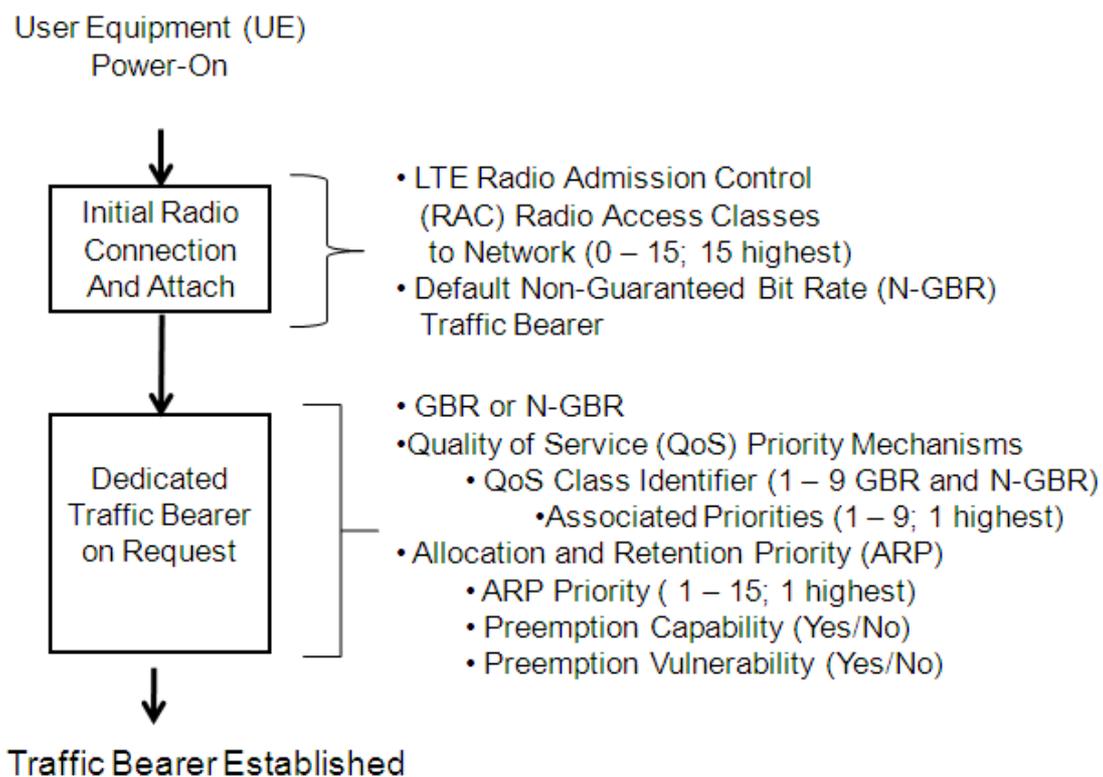


Figure 3.2: LTE/EPC Priority Management Mechanisms

After the initial steps of power-on, synchronization, and cell selection, the Random Access CHannel (RACH) procedure is invoked as a part of the Radio Admission Control (RAC) process. It is a key step in ensuring that priority enforcement is performed for admitting the higher priority public safety users. This procedure admits or rejects the establishment requests for Radio Bearer (RB) for control signaling as per the UE/ Universal Subscriber Identity Module (USIM) priorities (see Table A.2) [3GPP2, Sec.4.3.1], [3GPP6, Sec. 6.1.1].

The Evolved Packet System (EPS) bearer is the internal LTE/EPC bearer between the UE and the P-GW (See Figure 3.3) [3GPP10, Sec. 4.7.2] [3GPP16, Sec. 13.1]. It is segmented into the Evolved Radio

Access Bearer (E-RAB) and the core EPC S5 Bearer. There is a one-to-one mapping between E-RAB and EPC Bearer.

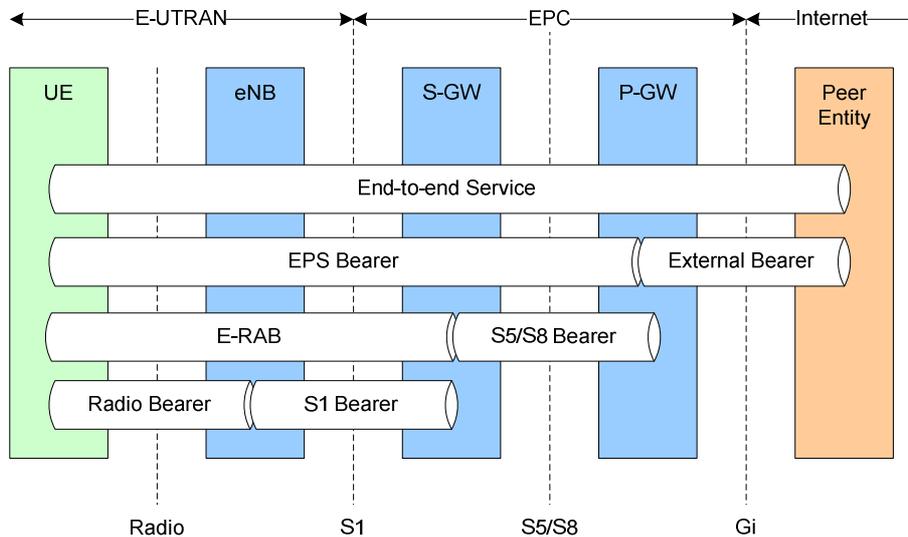


Figure 3.3: LTE/SAE Bearers [3GPP16, Fig. 13.1-1]

A typical traffic bearer is associated with a set of parameters to reflect the expected user experience defined in terms of Quality of Experience (QoE). QoE has been proposed as a concatenation of the traditional QoS concept along with user priority and application oriented parameters [PSCR1]. These additional parameters include authorized Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR) values, Aggregate Maximum Bit Rate (AMBR), Allocation and Retention Priority (ARP), and the QoS Class Identifier (QCI) [3GPP8, Sec. 6.1.7], [3GPP16, Sec. 13.2]. The application of the QCI and ARP mechanisms for priority management is summarized in Appendix A.

The overall priority treatment in an LTE-based network is implemented in the form of the Policy and Charging Control (PCC) process [3GPP9, Sec 6.1.5, Sec 7, Sec A.4], [3GPP10, Sec. 4.7.5], [3GPP12, Sec. 4.3]. The rules govern the bearer / IP - Connectivity Access Networks (IP-CAN) session establishment, modification, and termination. The process by which the PCRF gets its inputs and cooperatively works with the Subscriber Profile Repository (SPR), the Application Function (AF), and the Policy and Charging Enforcement Function (PCEF) is summarized in Appendix A.

3.3 Application of LTE Priority Mechanisms to Public Safety Users

The basic approach for the priority treatment for public safety users has previously been introduced in [ROBE]. It may be noted that although the 3GPP standards define the principles and mechanisms for priority management, specific implementations and designs can be vendor specific. This study will expand on the mechanisms that will be used to ensure that resources are always available to public safety users, even in the instance of severe congestion and an incident related urgent need for immediate public safety access to the data network. The intent of this study is to provide the basis for a common, agreed-on approach for priority access on shared networks.

The proposed priority management process in this study starts by identifying the community of users, their hierarchy and situation information, and the types of services followed by mapping these to the corresponding user priority, usage priority, and application types (see Figure 3.4). There are many possibilities for assignment [HALL], [PSCR3]. In this study, a representative mapping is proposed. This does not preclude other mappings at national or regional levels.

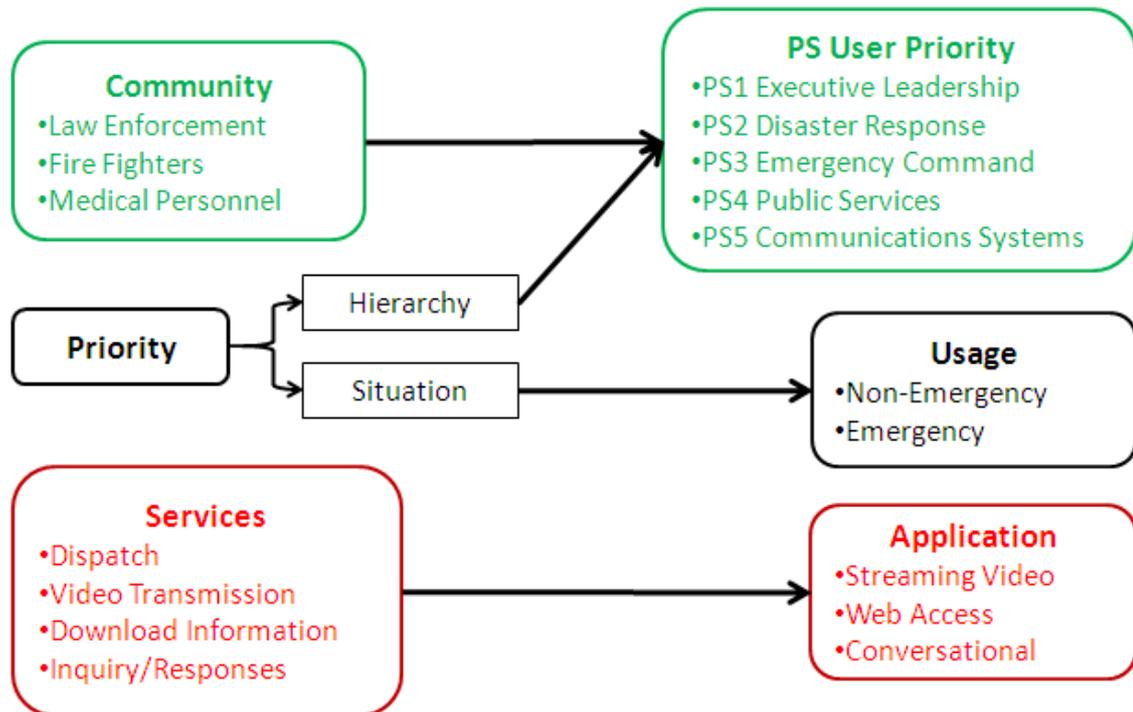


Figure 3.4: Representative User and Service Mapping Illustration

The priority for the radio access and attach process for initial access to the air interface and creation of the initial default bearer can then be assigned to the user priorities and usage (see Table 3.1).

Table 3.1: Radio Access Illustration

PS User Priority	User Identification	Traffic Class	Barring (RACH)	Establishment Cause (RRC)
	Reserved	15	BarringForSpecial	HighPriorityAccess
	PS Emergency (all)	14	BarringForSpecial	HighPriorityAccess
PS1: Executive Leadership	PS1: non-emergency	14	BarringForSpecial	HighPriorityAccess
PS2: Disaster Responses	PS2: non-emergency	13	BarringForSpecial	HighPriorityAccess
PS3: Emergency Command	PS3: non-emergency	13	BarringForSpecial	HighPriorityAccess
PS4: Public Services	PS4: non-emergency	12	BarringForSpecial	HighPriorityAccess
PS5: Communications Systems	PS5: non-emergency	12	BarringForSpecial	HighPriorityAccess

As illustrated in Table 3.1, public safety emergency usage (regardless of level) and the PS1 executive level in normal mode may be assigned level 14 keeping the highest level 15 reserved for network operator (internal) emergency messaging. The two remaining levels 13 and 12 may be assigned to the PS2 to PS5 users for normal mode operation. Also, access barring is designated “BarringforSpecial” so that the public safety users will not be barred from radio access even in congestion situation. Radio Resource Control (RRC) access establishment cause is designated “HighPriorityAccess”.

After radio connectivity has been established, the default non-GBR bearer is provided to the user. When a user attempts to initiate an application or a dedicated bearer, the ARP process is invoked and the corresponding bearer based on QCI values need to be established. Table 3.2 shows an example of application of the ARP priorities for public safety users.

Table 3.2: Allocation and Retention Illustration

User Identification	ARP Priority (1 highest)	Preempt Others	Preempt Vulnerability
Reserved	1	YES	NO
PS Emergency (all)	2	YES	NO
PS1: non-emergency	3	YES	NO
PS2: non-emergency	4	YES	YES
PS3: non-emergency	5	YES	YES
PS4: non-emergency	6	YES	YES
PS5: non-emergency	7	YES	YES

For public safety users, the six ARP priorities from 2 to 7 may be assigned for the public safety emergency and the PS1 to PS5 subscribers respectively, assuming that the highest ARP priority of 1 is reserved for the operator. The Preempt-others capability may be set to “yes” for all public safety users implying that in case of congestion, a public safety user would be able to preempt any other lower priority user, especially a commercial user. Preempt vulnerability may be set to “no” for class 14, i.e., public safety emergency and public safety executive, and “yes” for others in the public safety user group. This implies that in case of congestion, and if no other lower-priority commercial users are available for preemption, then normal mode PS2 to PS5 users may be preempted to allocate resources for the emergency PS or PS1 (executive) user. It may be noted that preemption in LTE does not necessarily imply termination of a user session.

The type of bearer assignment depends on the QCI value based on the application type. Table 3.3 identifies the QCI values and the corresponding priority that will be assigned by the scheduler for packet priority treatment in situations where the users in the system, public safety or others, are invoking three applications: Streaming Video, Web Access, and Conversational Voice.

Table 3.3: Application Bearer Treatment Example

Application	QCI Treatment	Priority (1 highest)
Conversational	1 (GBR)	2
Streaming Video	5 (GBR)	5
Web Access	9 (non-GBR)	9

It may be noted that a specific implementation may use mappings different from the ones recommended in the 3GPP LTE/EPC standards (see Table A.3). For example, for the three QCI values assigned for non-GBR data applications with their respective priorities of 6, 8, 9, one approach would be to assign them in an application oriented manner independent of the user type, e.g., QCI6, 8, and 9 to ftp, www, and email respectively. The ARP mechanisms will guarantee that the public safety users can utilize all allocated resources in case of congestion but the specific data applications will be restricted to their assigned QCI values. On the other hand, bearers may be assigned based on user priorities independent of the data application, e.g., QCI6, 8, and 9 could be assigned to high priority public safety users, “premium” users, and normal/commercial users respectively. This will restrict the public safety user to the higher priority level 6 for all data applications and the traffic will be scheduled at higher level as compared to the corresponding commercial users. Hybrid approaches are also possible.

The ARP parameters associated with a user are used by the various entities including the eNodeB, MME, and PCRF to provide the bearer assignment and retention. The priorities associated with the QCI values are embedded in the user packets. These may be mapped into the IETF defined DiffServ mechanisms for providing end-end-end QoS treatment [BROU].

So far, the attributes for public safety users have been addressed. The next section incorporates the presence of the commercial users into the mix and provides illustrative mappings for the total population.

3.4 Public Safety and Commercial Users in a Common Network

In order to extend the treatment summarized in Section 3.3 on public safety users to an environment where both public safety and commercial users are present, the commercial users (emergency and normal modes) may be allocated lower priorities.

Radio Access attributes mapping is summarized for both groups in Table 3.4.

Table 3.4: Radio Access for Public Safety and Commercial Users in a Shared Network

User Priority	User Identification	Traffic Class	Barring (RACH)	Establishment Cause (RRC)
PS First Responders	PS Emergency; PS1 to PS5	12 - 14	BarringForSpecial	HighPriorityAccess
Commercial User Emergency	Commercial User Emergency	10	BarringForEmergency	Emergency
Commercial User Non-Emergency	Commercial User Non-Emergency	0 - 9	Low BarringFactor	Mobile Originating

The resulting approach by which a public safety user is not blocked in accessing a shared network where commercial users may also be present is summarized in Figure 3.5. Appendix A provides further details of the mechanism by which the public safety users have access and commercial users are barred (delayed) during congestion situations using the System Information Block 2 (SIB2) mechanism [3GPP17, Sec. 5.2.2].

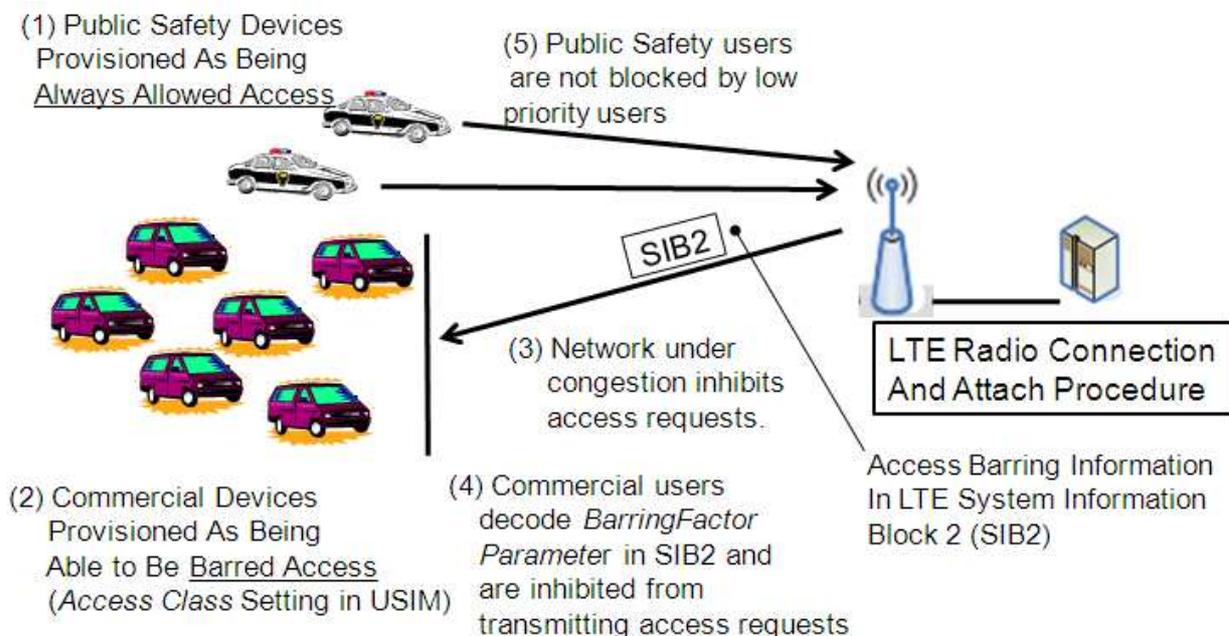


Figure 3.5: Public Safety Users not blocked under Congestion Situation

Also, it may be noted that during HO, a public safety user may be given higher priority during the RACH process via the use of a specific preamble.

In response to the “Handover Request” message, the target eNodeB may indicate the high priority RACH preamble to be used for non-contention based random access. During HO, the use of non-contention based random access by the public safety UE results in a higher probability of successful completion of the HO and a smaller handover delay. In case of a HO failure, the public safety user may be redirected to the public safety network and receive priority treatment consistent with its priority attributes.

Also, during HO, the PS_MME may send the target eNodeB a list of currently established bearers in the “Handover Request” message. This list includes the ARP associated with public safety bearers. The target eNodeB can consider the ARP when granting requests such that in times of congestion, public safety bearers, by virtue of their ARP priority level, will be given higher priority in the allocation process.

An illustrative bearer establishment mapping based on ARP attributes is summarized for a common environment with public safety and commercial users in Table 3.5. Again, many other alternate mappings can also be used.

Table 3.5: Allocation and Retention Approach for Mixed Users in a Shared Network

User Priority	APR Priority (1 highest)	Preempt Others	Preempt Vulnerability
PS First Responders	2 - 7	YES	YES/NO
Commercial User Emergency	8	YES	NO
Commercial User Non-Emergency	9 - 15	NO	YES

This implies that public safety traffic always gets through in the presence of the commercial users in a shared network environment (see Table 3.6)

Table 3.6: Public Safety User Bearer Priority Treatment

User Type		PS priority	ARP Preemption Priority	Can Preempt Others	Can Be Preempted
Public Safety Users	•Emergency		2	YES	NO
	•Priority 1		3		
Public Safety Users	•Priority 2-5		4-7	YES	YES/NO
Commercial Users (Emergency)	-		8	Yes	NO
Commercial Users	-		9-15	NO	YES

Public Safety Users
Can Preempt
Commercial Users
(in priority order)

Services mapping and application bearer treatment in this mixed environment are the same as before (see Table 3.3) since these are independent of the type of users.

The template can be applied to the situation of public safety and commercial users co-located in a network to illustrate how the public safety user gets the appropriate priority treatment in a mixed environment.

4.0 Assumptions and Shared Network Context

Some underlying assumptions required to support these scenarios need to be stated in several areas including operations and management, end-to-end treatment of the user traffic, and use of a specific application to illustrate the public safety priority management scenario. These assumptions allow us to describe the priority mechanisms in a concrete and simplified manner.

In this study, the emphasis is on the treatment of the public safety user in a dedicated home network to which HO and roaming of commercial users are not allowed, even if spare capacity is available. Technically speaking, this restriction can be readily removed, if desired. To complete the description of public safety and commercial user scenarios, the handling of the presence of the commercial user in the dedicated public safety network is summarized in Section 10.5.

A user of a public safety or carrier-grade communications system expects consistent end-to-end treatment for QoE. A typical end-to-end network consists of a set of entities which includes the access, core, backbone, and routing network. The end-to-end latency, for example, is budgeted into contributions for each of these entities. The layered security also needs to be treated in a similar fashion. For a typical end-to-end communication system, the IP-based packet transport infrastructure provides the key support for these attributes. A robust set of protocols and interfaces are provided by the Internet Engineering Task Force (IETF) including IPV4 and IPV6, Transmission Control Protocol (TCP)/ Internet Datagram Protocol (IDP), IntServ, DiffServ and IPsec among

others [IETF]. In this document, the discussion is confined to the QoE aspects and priority treatment associated with the access and core entities (LTE/EPC).

Similarly within the LTE/EPC complex, the bearer can be segmented into three major constituents: the Radio Bearer (RB), the S1 bearer, and the S5 bearer as shown in Figure 3.3. Only the RB is directly dependent upon the radio air resources and hence may be considered the bottleneck for resources. The backhaul (S1) between the eNodeB and S-GW, as well as the EPC internal S5 bearer between the S-GW and the P-GW, use hardware-based connectivity and use the processing power in the eNodeB, S-GW, and P-GW. These can be engineered such that they provide sufficient capacity even during emergency (high demand) situations. It is assumed that reasonable engineering design and capacity approaches have been applied so that the interfaces and various network entities do not become bottlenecks due to congestion. Hence, the primary focus in this study is the congestion situation associated with the RB and the study can be extended to the EPS if desired.

The various entities in the LTE/EPC complex may interpret the bearer capacity in terms of different attributes, e.g., bandwidth or frequency spectrum. The bearer in the LTE/EPC complex consists of an end-to-end concatenation of the RB, the S1 bearer, and the EPC bearer. The EPC and the S1 bearers can be primarily based on the use of bandwidth. For the RB, the bandwidth may not correlate directly with the frequency band since the adaptive modulation schemes for handling varying Signal to Noise (S/N) ratios and the scheduler operations make the bandwidth a statistically varying attribute. Hence for RB, a reasonable attribute may be the frequency resource block assigned to the user. In addition, the eNodeB uses several other second order parameters, e.g., the number of UEs or Number of Non-GBR bearers, for capacity limit calculations. The definition of the capacity is hence left at the discretion of the public safety agency and the commercial operator. The specific definition will not alter the conclusion of this study.

The focus of the authentication procedures in this study is user authentication and authorization, both of which have a direct bearing on the priority treatment for public safety users. As part of connecting to the network, there are other standard procedures such as the equipment identification check procedure carried out by the Equipment Identity Register (EIR) via the MME (S13 interface). That procedure is not explicitly covered in this document.

One key assumption is the co-location of the public safety and the shared commercial network wherein the radio frequency coverage area for the two cells is considered to be the same. The two cells for the public safety and the partnering commercial networks will operate in two different frequency regions. (Appendix B describes alternatives to this approach.) The HO for such networks can occur anyplace in the coverage area, and not necessarily at the cell boundaries. It may be noted that the traditional HO mechanisms in commercial networks are invoked at cell boundaries to mitigate weak signal conditions. The cell boundary HO to another network, e.g., to a neighbor public safety network, can be treated using the capabilities already provided in the 3GPP standards. In this study, the focus is on congestion conditions which require moving from the public safety network to the shared commercial network. Also, when capacity gets freed up in the public safety network, then a public safety user may be handed back to the public safety network to free up the resources on the commercial network.

Another key aspect for successful operation, especially for the public safety community, is the treatment of security. Security aspects, though mentioned in Appendix A, are not covered explicitly here since LTE/EPC provides a robust set of mechanisms for this purpose.

The LTE Release 8 (Dec 2009 version) standard is used as the base release since it is expected to be the one used in initial deployments. That release provides the underlying priority mechanisms for handling public safety users. This is also consistent with the demonstration network being constructed and analyzed by the joint NIST/NTIA effort [PSCR2]. Releases 9 and 10 augment the priority foundation set in Release 8 (see section 10.6.1 of this document). While the actual process of release upgrade is considered beyond the scope of this study, it will be important to develop a “roadmap” for priority access evolution so that consistency with future LTE releases is maintained, and enhancements in future releases can be used to advantage. Similarly, there are expected to be scenarios wherein different elements of the networks are operating on different releases. Making the assumption about a common release version at a particular instance in time is consistent with the underlying objective of this study.

The robust multimedia environment that LTE/EPC provides allows a user to invoke multimedia sessions, e.g., video telephony and ftp data transfer. The illustrative example used in this study is the streaming video application. For such real time applications including audio, HO can be accomplished with a discontinuous user data stream as long as the low probability of packet loss during HO is within the performance constraints of the end application. Section 10.4 summarizes the extension of the approach for data applications where continuity (no possibility of packet loss) of the data stream to the UE is maintained during HO. This is important due to the more stringent packet loss requirements for data applications. Real-time voice applications are also not specifically addressed in this study, since in the near future, according to the perspective of public safety [NYC], voice is expected to be provided by the current and planned narrowband public safety networks. The basic bearer assignment procedures available in the 3GPP standards, particularly the QCI framework, allow robust priority treatment for multimedia environments.

This study provides a method for the application of the priority management for public safety users in a dedicated public safety and the shared commercial network environment. It is intended to provide a base for further discussion and refinement. It is expected to be a starting point for a single, definitive approach for priority access for public safety on shared commercial networks. The intent is not necessarily to suggest an optimum solution or to design a final implementation. There may be modifications to the approach described here that result in less complexity and cost. It is expected that the vendors and the operators will carry out the necessary diligence to develop optimized solutions for the benefit of the public safety community.

5.0 Public Safety and Shared Commercial Network Solution

In section 5.1, three architectures are proposed to illustrate how the public safety user priorities can be managed regardless of whether the public safety user is in the dedicated public safety network or the shared commercial network. The detailed analysis is carried out for a

representative architecture which allows focused control by the public safety agency for public safety user management and traffic. The analysis is extended to the other two additional architectures in Section 9.

Section 5.2 provides augmentation and translation of the high level public safety user requirements to a set of specific requirements based on the architecture chosen.

Subsequently, the application of the LTE/EPC attributes to the public safety and commercial users is covered since both will co-exist in the shared commercial network. The corresponding impact and support needed from the various network elements both in the dedicated public safety network and the shared commercial network are also addressed.

5.1 Representative Shared Network Architectures

The following representative architectures for the dedicated public safety and the shared commercial solution are proposed:

- Separate public safety and commercial RANs connected to the public safety EPC core.
- Shared RAN Architecture.
- Independent public safety and commercial networks.

Figure 5.1 shows the architecture for the public safety and shared commercial networks with separate RANs. The intent is to provide the public safety organization comparatively direct control over the resources and management of the public safety user and the public safety user traffic.

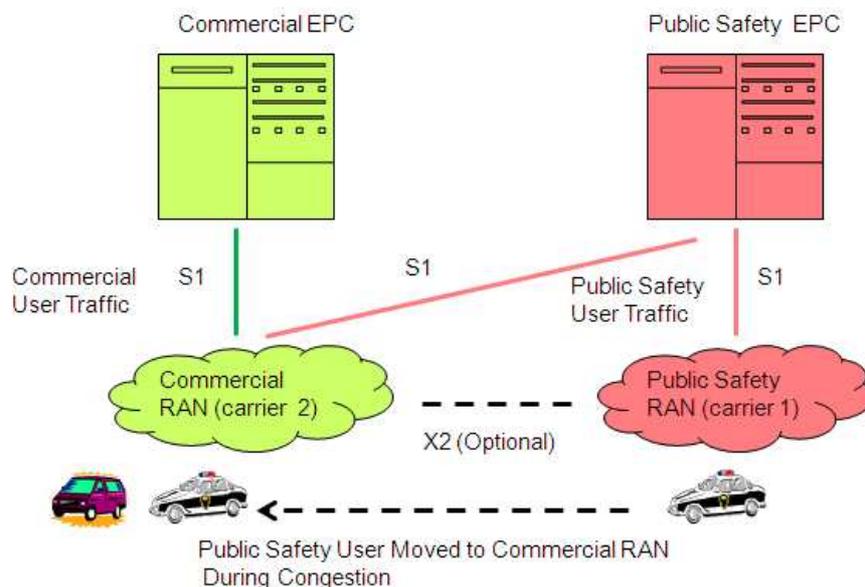


Figure 5.1: Both RANs Connected to Public Safety EPC

The public safety traffic is initially supported in the public safety RAN at carrier frequency C1. During congestion situations, the public safety user is handed over to the shared commercial RAN, but the public safety user traffic continues to be directed to the public safety EPC via the S1

interface. The commercial users can only connect to the commercial RAN and their traffic is directed through the commercial EPC. The functionality and attributes of this architecture are described further in Appendix B.

Another shared approach involves the use of a common eNodeB which operates on both the dedicated public safety spectrum block and a shared commercial partner frequency band. Figure 5.2 illustrates an example of the 5MHz public safety band paired with a commercial 5 MHz band.

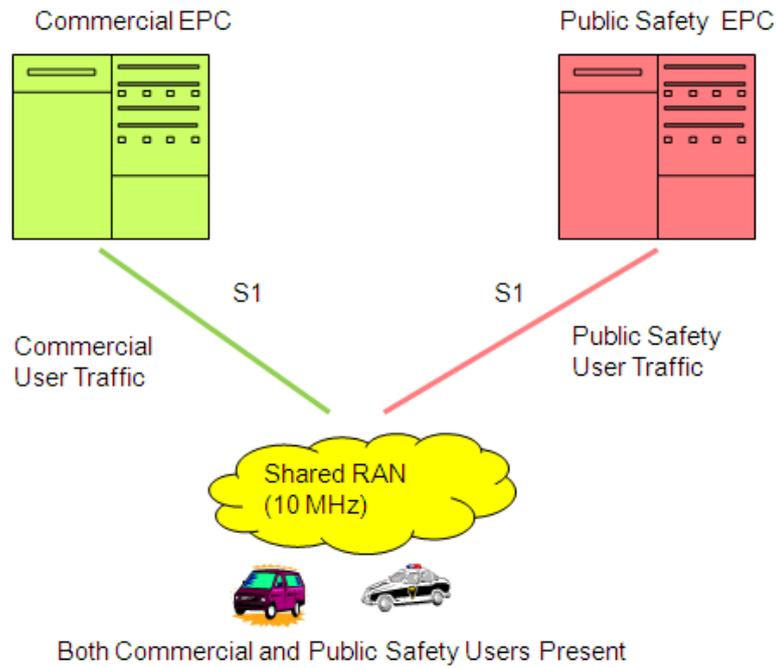


Figure 5.2: Shared RAN Architecture

The eNodeBs direct the commercial and public safety user traffic to the respective EPCs. The operations and attributes are described further in Appendix B.

In the third architectural option, shown in Figure 5.3, the public safety and the commercial RANs are connected to their respective EPCs.

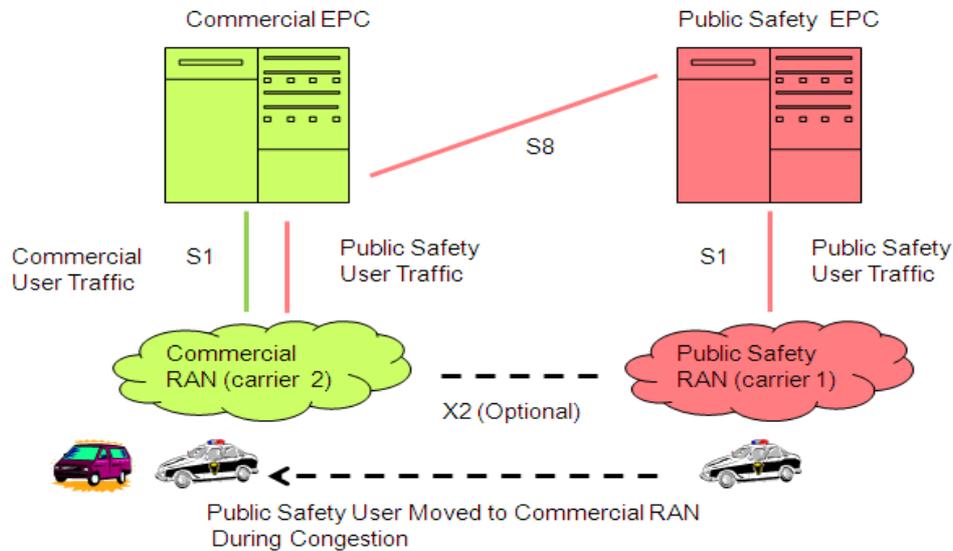


Figure 5.3 Independent Public Safety and Commercial Networks

While in the commercial RAN environment, the public safety user traffic utilizes the S1 interface to the commercial EPC. However, public safety user traffic may still be directed through the public safety P-GW. The commercial RAN, MME, and S-GW are engaged in handling the public safety traffic. Appendix B provides additional discussion on the operations and attributes of this architecture.

5.2 Requirements for Public Safety and Shared Network Environment

In this section, the overall requirements as expressed by the public safety entities and summarized in Section 2 are augmented and applied to the architecture shown in Figure 5.1. The requirements summarized in this section will be used in the subsequent sections to show how this dedicated public safety and shared commercial architecture provides a robust priority management solution to the public safety users, regardless of whether the public safety user is in the dedicated public safety RAN or the shared commercial RAN.

Also, as stated in the assumptions in Section 4, the resources in the core EPC network and the S1 backhaul are considered to be properly engineered. Therefore, the focus of the requirements will be on the Radio Bearer (RB) resources. For initial analysis, commercial users are restricted from connecting to the public safety dedicated network.

In order to treat the requirements in a structured and consistent manner, they are evaluated in three categories: general requirements, Hand Over (HO) at cell edges to another public safety network, and HO due to congestion into shared commercial network.

5.2.1 General Requirements in Shared Environment

The general requirements, and an explanation of them, are presented in this section. The requirements pertain to the priority management of the public safety user while in the home public safety RAN or after HO to the shared commercial RAN.

The public safety user shall have radio access to the public safety and the commercial RAN even under congestion situations.

This implies that enough public safety and commercial RAN control channels are available for initial connectivity to be established for the public safety user in either of the RANs. This is provided for during the system design process. As discussed in Section 3.4, commercial UEs can be blocked or delayed from accessing the control channels under periods of extraordinarily high demand, so that public safety users can establish an initial connection to the network.

Regardless of overload situation in the public safety RAN, the public safety UE will first attempt to connect to the public safety network (home or visited).

This requirement ensures that the initial access and assignment treatment for the public safety user will be in the public safety RAN network. To meet this requirement, the Public Landline Mobile Network (PLMN) ID or the equivalent of the Neighbor Cell List (NCL) will be programmed in the PS_UE to facilitate public safety LTE network as the primary choice. The public safety user will move to the commercial network only if the public safety network is congested. A congestion condition in the public safety network implies that either all radio resources are utilized or the remaining marginal resources are not sufficient to meet the new request. The new request may be for a bearer for a public safety user when a new public safety user attempts to connect or when an existing public safety user requests additional resources.

In the event that the network bandwidth in the public safety portion of the network is not available or is congested, the network must provide a mechanism to accommodate public safety users by preempting commercial users [NPST1].

One of the constraints being used in this study is that the commercial users are not allowed in the public safety RAN. Therefore, congestion in the public safety RAN will only occur due to public safety user congestion, not commercial user congestion. Even in the shared environment, this is not intended to be the “ruthless preemption” as in classical circuit-based systems. The LTE priority mechanisms as discussed previously provide mechanisms for preemption, and an operator may choose to provide preemption treatment in the form of reducing performance and keeping the functionality, or alternatively, handing over the user to a different network.

The commercial RAN will support both the visiting public safety users and the home commercial users and the priority for public safety users will be higher than for commercial users.

This ensures that the public safety user will get higher priority treatment as defined by the public safety organization even if the public safety user is moved to the shared commercial RAN during congestion conditions in the public safety RAN.

The move into the commercial network will be automatic and transparent to the public safety user.

The public safety user does not need to take any action when congestion conditions occur in the public safety RAN. The public safety UE is handed over to the partner commercial network based on the NSA between the public safety entity and the commercial operator. In addition, such a move will be handled by the PS_eNodeB, the PS_MME, and the C_eNodeB without requiring any operator action from the public safety or the commercial Operations, Administration and Management (OA&M) console.

The commercial network must be able to distinguish between public safety traffic and commercial user traffic [OIC].

The C_eNodeB in concert with the PS_MME and PS_eNodeB will be able to discriminate between the traffic originating or terminating with the PS_UE or the C_UE and direct them to the PS_S-GW and the C_S-GW accordingly based on the association of a UE with its bearer.

Depending upon the agreement between the public safety agency and the commercial operator, a public safety usage limit PS_max_capacity, e.g., max%, will be defined.

This limit value can be dynamically modified by the commercial operator through the C_OA&M upon request from the public safety agency. This request may be triggered either automatically under pre-defined criteria and emergency conditions or will require a request from the public safety organization representative to commercial organization personnel.

For default automatic operation, the total resources assigned to the public safety users in the commercial network will be limited to this pre-defined value. This limit value could be anywhere between “zero” and “100%” based on the agreement between the two organizations. In the 0% condition, public safety UEs are not allowed to use the shared commercial RAN resources. In the 100% condition, all commercial RAN resources are available to the public safety user equipments with the commercial users subjected to lower priority treatment.

The data relating to the use of the allocated capacity in the commercial RAN by the public safety users will be automatically provided to the public safety agency and available on the public safety OA&M console.

The public safety UE will use the commercial C_eNodeB and S1 resources. The PS_UE usage data in the commercial entities needs to be captured for subsequent reconciliation between the public safety agency and the commercial operator based on the NSA.

Mechanisms must be available to automatically identify public safety personnel when the public safety user moves into the commercial network.

The C_eNodeB must support the priority treatment for the public safety user and it must be able to identify a public safety user when it moves into the shared commercial domain.

Three possible scenarios can be considered:

1. Both Public safety network and shared commercial network exist.
2. Public safety network exists and commercial network does not exist.
3. Public safety RAN does not exist, or is non-operational, and commercial network exists.

In the following, the treatment for the public safety users is summarized for these situations.

1. Both public safety network and shared commercial network exist.

The overall treatment is summarized in Figure 5.4.

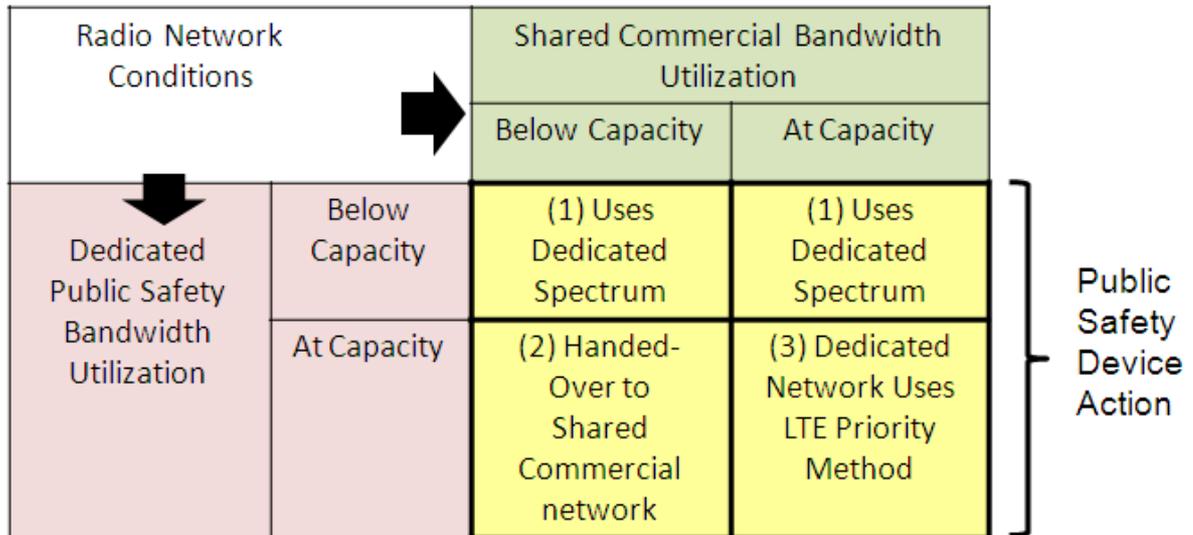


Figure 5.4: Public Safety User Equipment Operation

- a. Public safety network is not congested.

The upper row (1) corresponds to the situation wherein the public safety RAN is not congested and the commercial RAN may or may not be congested. The public safety UE gets its resources in the normal fashion in the public safety RAN.

When a public safety user initiates connection, normal treatment to set up the connection and the user data traffic bearer is undertaken in the public safety network. Similarly, if an existing public safety user equipment requests additional resources, then a dedicated bearer is created with higher resource levels. In either case, there is no impact on existing public safety users.

- b. Public safety network is congested and shared commercial network is not.

The lower left corner (2) indicates the situation in which the public safety RAN is congested, but there is capacity in the commercial RAN for the public safety user. The public safety UE will be moved to the commercial RAN.

When a new public safety UE requests additional resources (dedicated bearer), then that UE is directed to the shared commercial network regardless of the priority level associated with the new user. There is no impact on other existing public safety users in the public safety network. If an existing public safety UE requests additional resources, then a lower-

priority-level public safety user is automatically transferred to the shared commercial network.

c. Public safety and the commercial networks are congested

The right lower corner (3) implies both the public safety and the commercial RANs are congested. In that case, resources are freed up for a new or existing public safety user requiring additional resources by preempting a lower priority public safety user in the public safety RAN.

A new public safety UE may require a bearer set up, or an existing public safety UE may request additional resources. In this situation, the new or requesting public safety UE will be handled in the public safety RAN and priority mechanisms for the public safety users will be invoked in the dedicated public safety network. A “lowest” priority public safety user will be identified in the public safety network to be preempted to free up the resources for the higher priority public safety user.

LTE “Preemption” may be treated as the following precedence of actions:

1. The resources for the lower priority public safety users may be reduced, e.g., CODEC rate reduction while still keeping the functionality of the service, albeit at lower performance
2. The lower priority user may be handed over to another neighbor network

It may be noted that only in extenuating circumstances, an existing user may be dropped as the result of preemption.

If no other lower priority user is available for preemption when a new or existing public safety UE needs resources, then the requesting UE will be handed over to another network, if available.

2. Public safety network exists and commercial network does not exist.

In this situation, standard priority treatment is applied in the public safety network. In case of congestion, priority mechanisms will be invoked as indicated above in the public safety network.

3. Public safety RAN does not exist, or is non-operational, and commercial network exists.

It may be noted that any user, including a public safety user, needs to have a home network where the subscriber information resides. This information needs to be available to a visiting network to provide service to the visiting public safety user. This is expected to be a frequent and important case especially in rural environments, where the commercial network may exist, but a public safety network may not exist in the same coverage area. As part of the NSA, it is necessary that access to the PS_HSS and PS_PCRF is available to the visitor network to support the public safety user.

In this case, the public safety UE will be able to connect / roam into the visited commercial network subject to the NSA between the public safety organization and the commercial operator and will be able to invoke the priority requirements. The NSA may include a maximum capacity that the public safety UE may be allocated in the visitor network.

5.2.2 Hand Over at Cell Edges to another Public Safety Network

In this section and the next, the requirements relating to the HO at the cell edge and capacity congestion in the public safety network, are highlighted.

At the cell boundaries, with weak signal strengths for both the source public safety and the shared commercial network, the HO procedure will be invoked for mobility into the adjacent public safety network (not to the overlapping commercial network).

The scenario for a public safety user HO to another public safety network is not covered in depth in this study since it is not the focus of the study, but the proposed approach could be directly applied to this situation as well.

A public safety user expects the same priority treatment in a visitor public safety network as in the home network. Note that the LTE standards recommend that a visitor roaming or being handed over to a network may be given lower priority than a user in its own home domain. This is generally applicable for commercial users. It is left to the discretion of the public safety agencies to decide the relative priority handling approach for the home and visiting public safety users.

If the target public safety network is at its capacity limit, then HO to the “stronger” shared commercial network will be explored, if available.

5.2.3 Hand Over due to Congestion into Shared Commercial Network

If the public safety network reaches its capacity limits and a new public safety UE requests services, the control signaling responsibility will be transitioned to the commercial RAN and the traffic bearer will be set up with the public safety EPC.

In the shared commercial RAN, the public safety user will be given the access connection in preference to incoming commercial users.

When a public safety person moves into the shared commercial network, the transition will occur without requiring public safety user intervention.

When the public safety user moves into the commercial RAN, the non-emergency or the emergency/priority mode will be preserved. Equipment will be reconfigured to switch to the new network automatically as a default.

The commercial eNodeB will provide allocated capacity to the public user in its capacity domain. If there is spare capacity not being used by the public safety users, then that spare capacity can be used by the commercial users.

Section 5.3.1 describes in detail how a guaranteed level of capacity on the commercial network can be reserved for public safety users. This pre-set level of guaranteed capacity would be negotiated as part of the sharing agreement between the public safety governing entity and the commercial operator. Extending the public safety capacity on the commercial network beyond the pre-set level can be accomplished if necessary. Real-time human intervention from the commercial console in the shared commercial network to facilitate additional resources will be allowed so that priority-related decisions can be based in part on situational information that the system cannot detect on its own, such as the intention of public safety use or request from the public safety organization under emergency conditions. This is of particular significance to the public safety users. The primary action entails modifying the public safety usage allocation limit value from the commercial console. This may be triggered by an explicit request from the public safety agency or an automatic indication from the public safety network to the commercial network especially during emergencies.

If the allocated public safety spare capacity in the shared commercial network is being used by the commercial users then

- *New commercial users will be blocked (or delayed) from accessing the commercial RAN or handed over to another partner commercial network.*
- *Existing commercial user(s) will be preempted in case of arrival of a new public safety user.*

Preemption, as indicted previously, may not normally result in dropping the user session.

If the public safety and the commercial users are both using their allocated capacity,

- *The public safety user will receive the priority treatment in its own public safety RAN unless an increase in capacity on the commercial network is made available for public safety users.*

Figure 5.5 captures a typical scenario for a public safety user connection based on these requirements. The advantages of the resulting public safety / commercial partnership have been summarized in [NEWM].

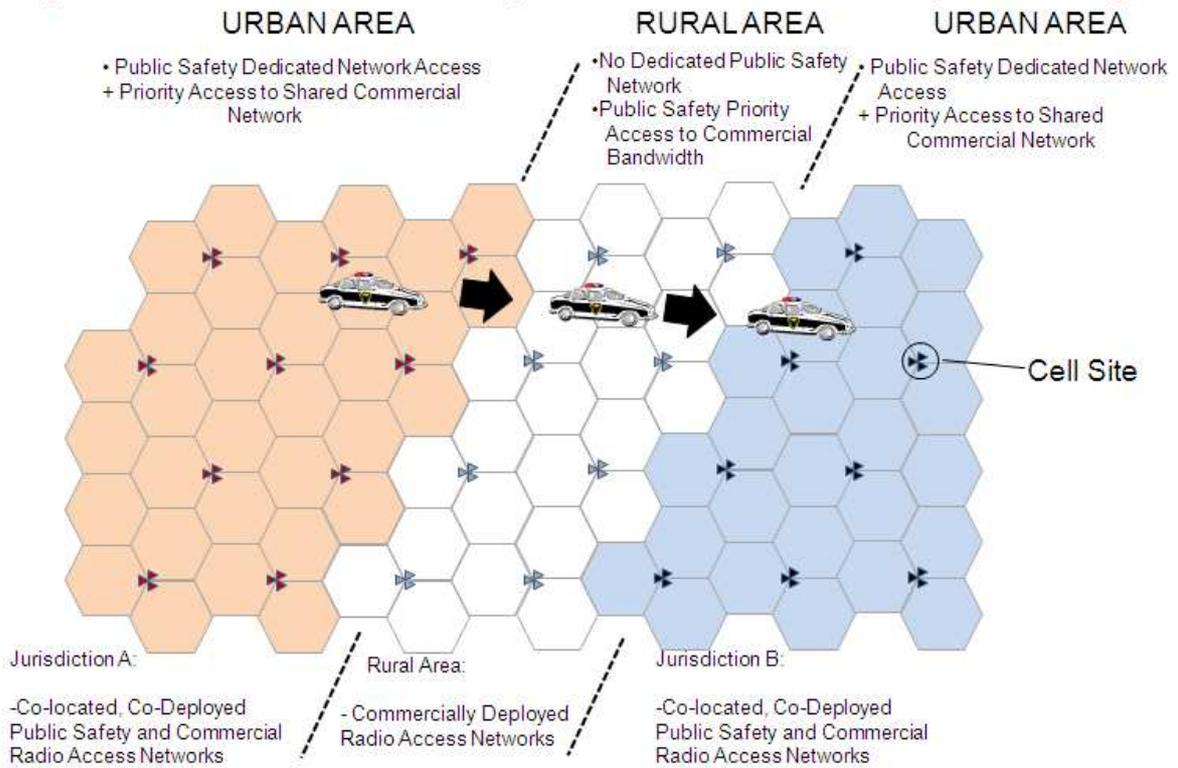


Figure 5.5: Public Safety Broadband Interoperability

Urban area jurisdictions A and B have co-located, dedicated public safety and shared commercial networks. The public safety user would expect initial access in the dedicated public safety network and HO to the shared commercial network with the same priority treatment as in the public safety network. In a typical rural area, only a commercially-deployed network may exist, but the public safety user still needs to get the similar priority treatment. In such a case, the options of the Local Breakout or the Home Routed roaming scenarios, as indicated in Appendix F, may apply where the visited commercial network communicates with the public safety user's home public safety network to provide appropriate priority treatment. In addition, as the public safety user moves from one zone to another, HO may be needed.

The resulting roaming and HO scenarios are summarized in Figure 5.6.

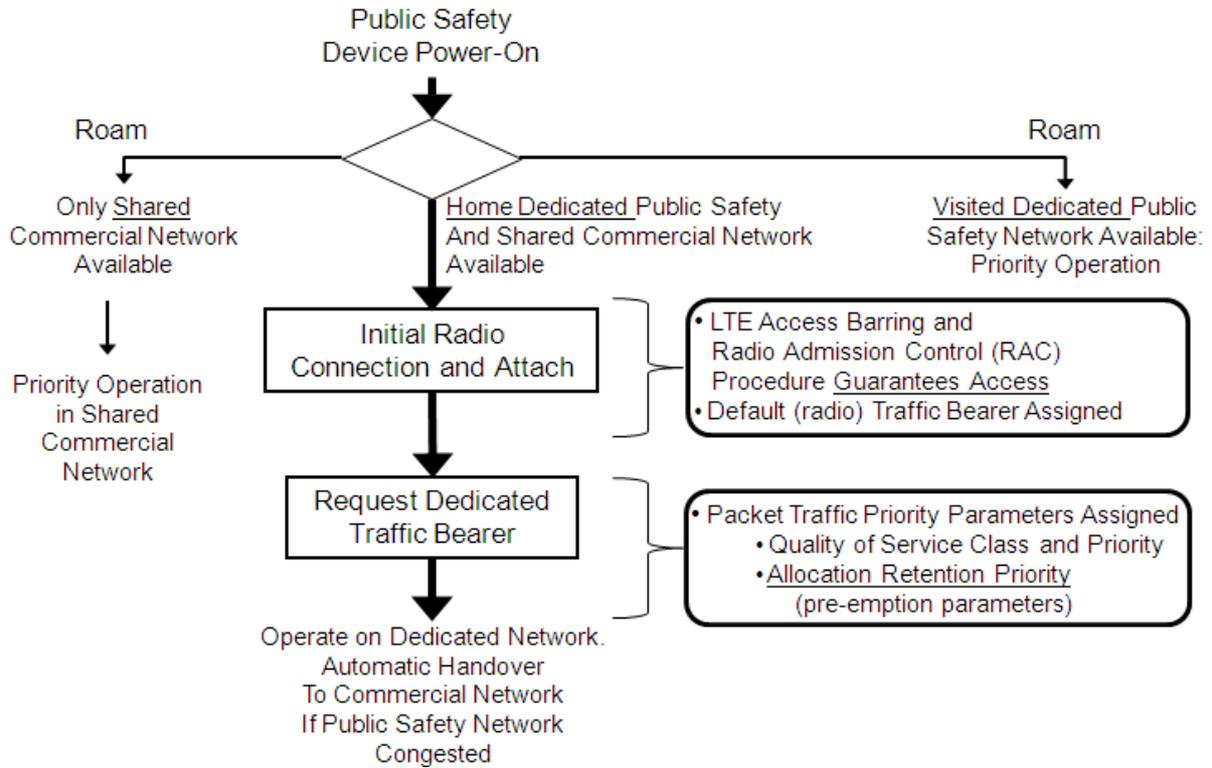


Figure 5.6: Network Interoperability and Equipment Startup

In rural areas, or other jurisdictions where a dedicated public safety network may not exist, the public safety user needs to have priority treatment in a shared D-block or other commercial network via roaming support. Similarly, if a public safety user is visiting a network other than the home public safety network, then the roaming process applies. The middle path shows a home public safety network co-located with a shared commercial network. This study is focused on this scenario. Other situations, and treatment in other technologies, are presented in Section 10.

5.3 Implications on Public Safety and Shared Commercial Networks

The requirements in Section 5.2 require that specific capabilities be supported by the network elements in addition to the basic implementations as defined by the 3GPP standards. Application-level software may need to be developed to run on these elements along with the priority management-oriented rules

5.3.1 General

The key elements that participate in priority management for the public safety users are indicated in Figure 5.7 for the architecture in Figure 5.1.

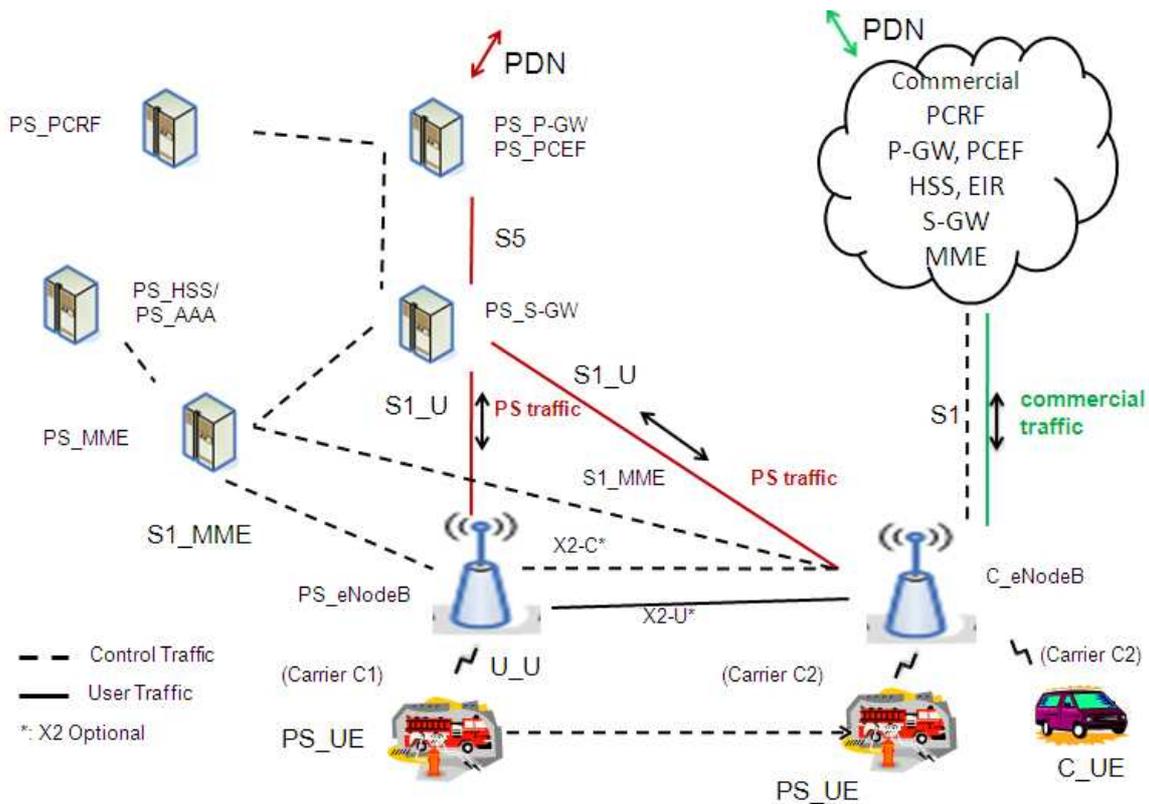


Figure 5.7: A Representative Dedicated Public Safety and Shared Commercial Architecture

The PS_eNodeB and the C_eNodeB operate on two separate 5 MHz C1 and C2 carriers respectively. Both eNodeBs have a common coverage area and sectoring approach.

The PS_UE operates on both the public safety carrier (C1) and commercial carrier (C2) network whereas in this example, the C_UE is allowed to operate only on the commercial carrier C2 in order to restrict it from moving to the PS_eNodeB. Upon connection request, the PS_UE is connected to the public safety RAN as a default instead of commercial RAN. This is done via use of the “priority-based scheme” [3GPP16, Sec. 10.2.4] in the UE which allows a set of frequencies (and technologies) to be priority ordered so that the UE may select its primary RAN to be connected to. The co-located commercial RAN is also part of the neighbor list for the PS_UE and the PS_UE makes the measurements for the commercial RAN and reports them to the PS_eNodeB as part of the preparation for a possible HO to the commercial RAN.

All control and user traffic for the PS_UEs in the C_eNodeB use the S1 interface to the PS_EPC and utilize the PS_MME, PS_HSS, PS_S-GW, PS_P-GW, and PS_PCRF.

The total bandwidth resource capacity of the PS_eNodeB is dedicated for use by the public safety users. To account for congestion situations, the public safety users are “allocated” certain amount of resource / capacity in the shared commercial RAN, up to a limit value PS_max_capacity (see Figure 5.8). This needs to be part of the NSA between the public safety agency and the commercial operator and could be 0%, i.e., no public safety user allowed in commercial network to 100%,

wherein potentially, the C_RAN may allow the public safety users to use the total capacity of the commercial RAN based on the priority mechanisms under emergency conditions.

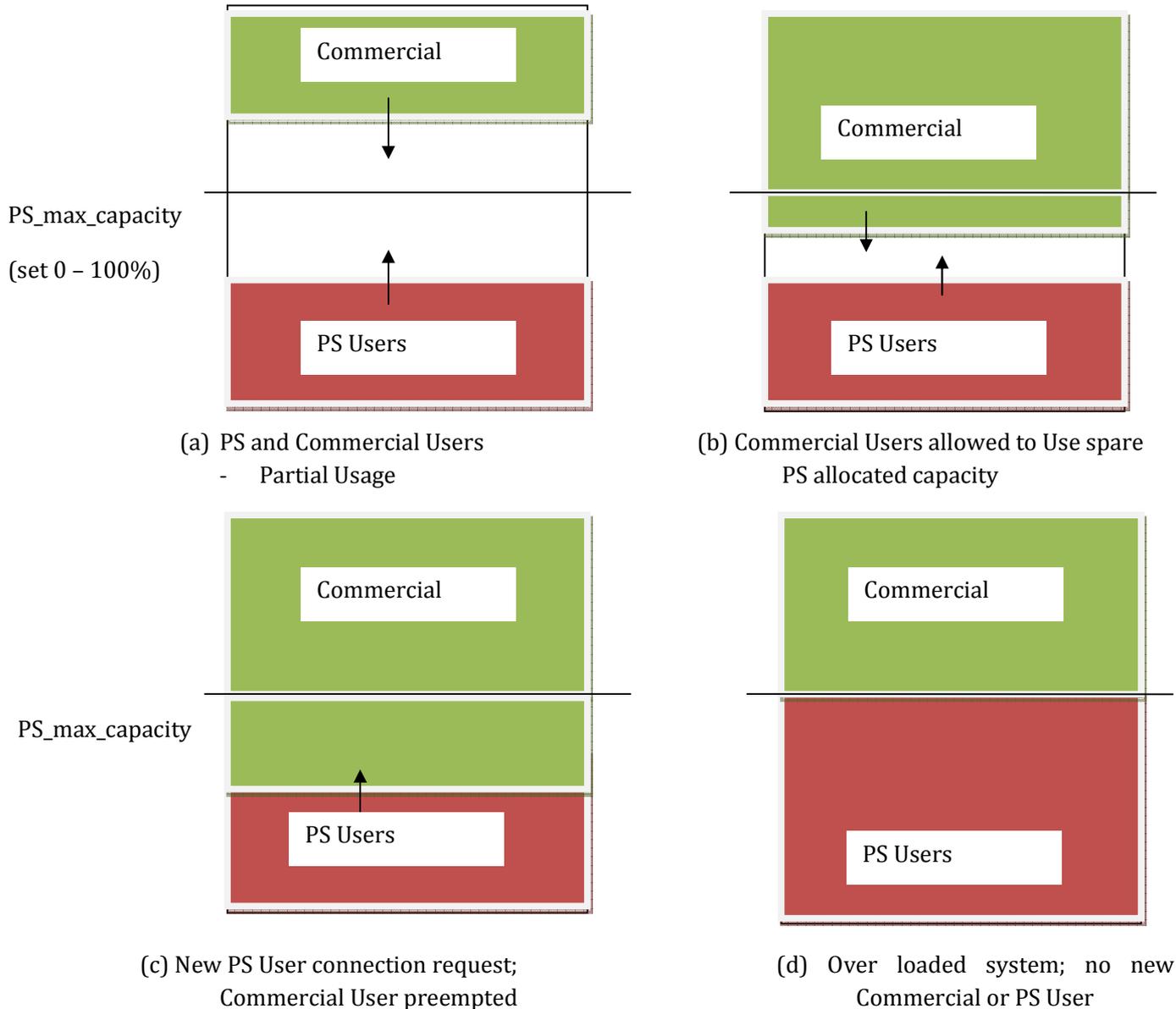


Figure 5.8: Commercial RAN Public Safety and Commercial Usage Scenarios

It is expected that at most times, the public safety users may not be using the allocated capacity in the commercial network. In order to use the commercial network at maximum capacity for commercial users without compromising the public safety priority treatment, the spare public safety allocated capacity may be used by the commercial users.

Figure 5.8a shows the situation in which there is spare capacity for both the public safety and the commercial users in their respective allocated domains in the commercial eNodeB and normal bearer assignment mechanisms operate. Both the public safety users directed from the congested

public safety RAN and new commercial users can be accommodated in the shared commercial RAN with no contention.

The situation in which the commercial users have exhausted their capacity range, but there exists spare capacity in the public safety allocated region is shown in Figure 5.8b. Additional commercial users can be supported so that the scarce spectrum resource is effectively utilized without compromising the public safety user priority requirements. The C_eNodeB and the C_MME will manage the commercial users in the spare public safety allocated capacity space.

The maximum range to which the commercial users can penetrate is shown in Figure 5.8c. In this case, if a new commercial user needs resources, that user is rejected since priority based preemption of users is not practiced for commercial users. However, if a new public safety user is handed over from the PS_eNodeB due to congestion in the PS_eNodeB, then, in the public safety allocated domain of the C_eNodeB, the public safety user is given higher priority and a commercial user may be preempted. This is consistent with the notion of the public safety allocated capacity in the commercial RAN. The C_eNodeB and C_MME handle the treatment for the commercial users which may include reducing the allocated resources or handing over to another commercial eNodeB in its jurisdiction.

Figure 5.8d shows the total capacity utilization scenario wherein both the public safety and the commercial users have utilized their respective maximum allocated capacities. A new commercial user is not allowed to connect to the C_eNodeB and may be handed over to another commercial network. A newly arriving public safety user from the congested PS_eNodeB also cannot be supported in C_eNodeB. One approach would be for the new public safety user to preempt another lower priority public safety user in the C_eNodeB. Although this can be supported as well, the strategy of keeping the new public safety user in the congested PS_eNodeB and applying the appropriate priority treatment in the PS_eNodeB by preempting a lower priority public safety user is preferred. This allows preemption for the lower priority public safety user to be managed directly by the public safety network.

It may be noted that when the public safety user traffic has reached the maximum allocated capacity in the C_eNodeB, the public safety user is not allowed to use the commercial capacity even if it is available, in keeping with the spirit of the public safety maximum allocated limit framework. Note that if the public safety users were allowed to use the region beyond the public safety allocated space, then subsequent commercial users would be blocked in their own space since they cannot preempt a public safety user. The capacity limit for public safety can of course be modified in real-time if necessary upon agreement between the public safety agency and the commercial operator.

In summary, the maximum capacity available in the C_eNodeB from the public safety user perspective is the capacity “A” shown in Figure 5.9. The capacity available in the C_eNodeB from the commercial user perspective is the capacity “B” and it can vary dynamically.

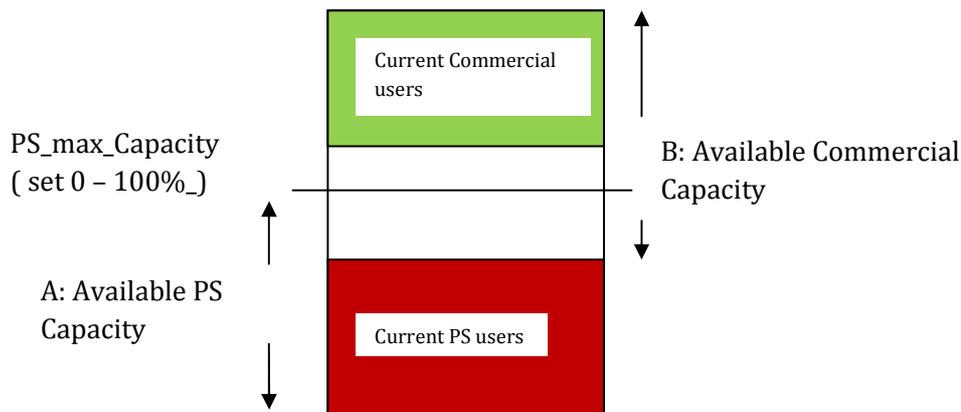


Figure 5.9: Available capacity for Public Safety and Commercial users in the Shared Commercial eNodeB

From the PS_MME and PS_eNodeB perspective, the overall maximum public safety user available capacity = PS_eNodeB Capacity + PS Allocated capacity in the shared commercial C_eNodeB.

From the C_MME and C_eNodeB perspective, the maximum commercial user available capacity = Total Commercial eNodeB Capacity

In the overlapping region A in Figure 5.9, the public safety user gets higher priority treatment as compared to the commercial user. After a public safety user is moved to the C_eNodeB, then neither control nor traffic bearer resources are applied for it in the public safety RAN. The Priority treatment for the public safety users is not performed on an incident-to-incident basis, but rather is based on the standard public safety priority treatment as defined in the PS_PCRF as long as they are in the commercial network within their pre-defined allocated domain. The priority treatment is consistent with the treatment defined for emergency or normal operations.

The usage data for the public safety user whether in the public safety RAN or in the commercial RAN is logged in the public safety OA&M system. These may include the standard data collected for a user along with data relating to:

- Successful connection in the dedicated public safety RAN.
- Attempts to move to the commercial RAN.
 - Successful ones.
 - Redirected ones back to the public safety RAN.
- Successful connections in the commercial RAN.

5.3.2 Impact on Network Elements

The architecture chosen, and the allocation limit approach in the previous section, require certain priority management-oriented capabilities. The public safety RAN and core networks are involved in the priority management of the public safety user while the public safety user is in the public safety RAN or the commercial RAN. The commercial eNodeB and the EPC are responsible for managing commercial users. The commercial eNodeB cooperates with both the public safety core and the commercial core. This section highlights the impacts on these network elements.

5.3.2.1 Public Safety Network Elements

The public safety RAN and core elements, i.e., PS_eNodeB, PS_MME, PS_HSS, PS_S-GW, PS_P-GW, and PS_PCRF, hold the data and manage the activities only for public safety users. They are not involved in any commercial connection or traffic handling. Standard public safety user handling and priority-treatment-related support is provided.

As indicated in Section 3.4, the public safety user undergoes two major steps as part of establishment of a traffic bearer: 1) the initial radio connection and attach and 2) the establishment of a (dedicated) radio bearer (see Figure 5.10). Various elements play their role in supporting such activities.

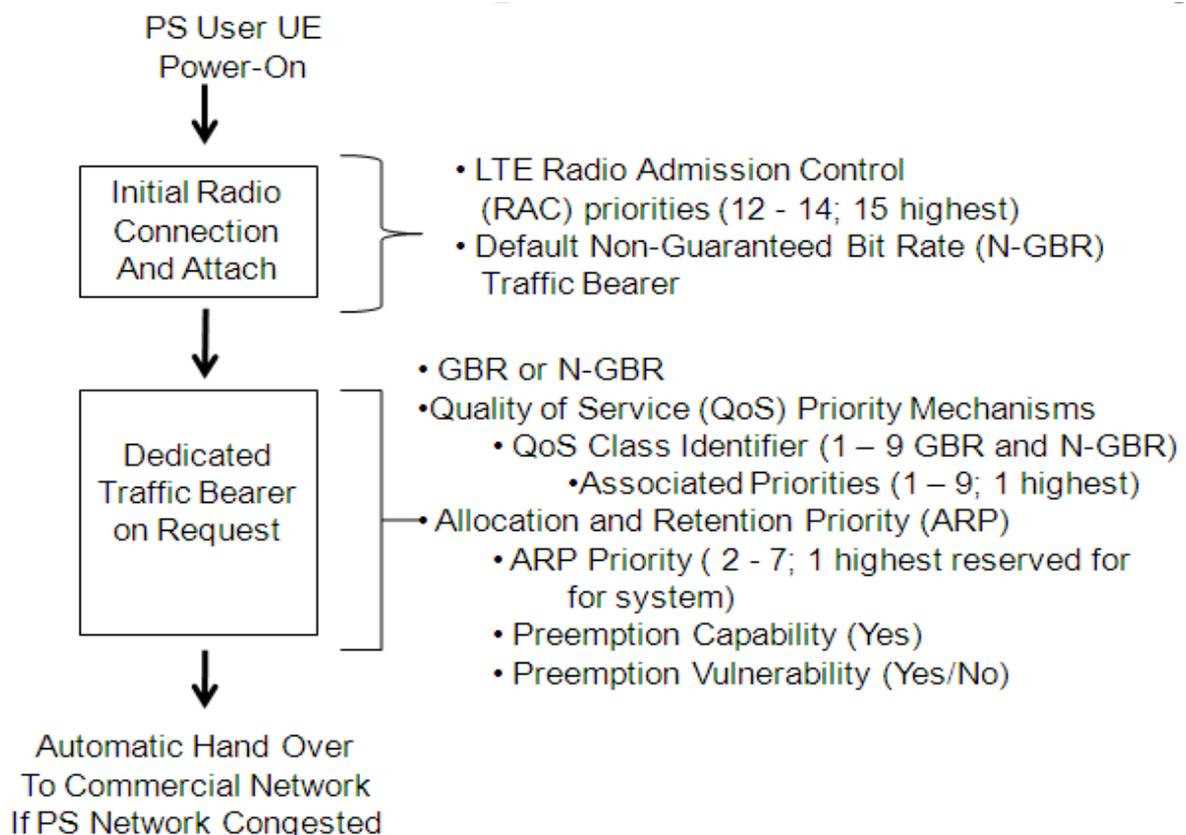


Figure 5.10: Priority treatment for Public Safety User

The PS_eNodeB plays a key role in radio admission and bearer setup. The PS_eNodeB has the PS_PLMN ID populated. An eNodeB has the capabilities to deny accessibility to any UE in order to handle maintenance or operator emergency situations. In order to also allow ONLY public safety emergency calls (regardless of public safety user priority) and public safety executive leadership calls for all situations, the cell reserved attribute may be set to “cell reserved not enabled,” consistent with the access class of 15 for such users. A rudimentary activity chart based on how admission control may be established for a public safety user [3GPP16, Sec. 13, 16], [3GPP13, Sec. 6], is provided in Appendix C.

The PS_MME and PS_S-GW provide the S1 interface (S1-MME and S1-U) support to the public safety user whether in the PS_eNodeB or the C_eNodeB. PS_MME directs the public safety traffic through the PS_S-GW and PS_P-GW in collaboration with the PS_PCRF. Note that the source PS_eNodeB and target C_eNodeB are the primary entities responsible for the HO process and have the necessary load data to take HO decisions.

The overall procedures for PS_MME are the standard ones as they apply to all users since it works with PS_eNodeB and PS_HSS for subscriber attach and bearer assignments. Its primary role is attachment, bearer setup, and mobility management [3GPP15, Secs. 5 and 6]. During HO to the shared commercial network, the role of the PS_MME depends upon the type of HO used.

As indicated in Appendix A, there are two primary choices for HO between LTE RANs: the X2 based HO when the X2 connectivity is present between the source eNodeB and the target eNodeB, and the S1 based HO which is applicable when the X2 interface between the source and the target eNodeBs is not configured. In case of X2 based HO, the PS_eNodeB is the one responsible for the HO activities and the PS_MME assists the HO process in the final stages in directing the PS_S-GW to switch the S1-U bearer path from the source PS_eNodeB to the target C_eNodeB. In case of S1 assisted HO, the PS_MME is primarily a pass-through for the communications between the source PS_eNodeB and the target C_eNodeB during the HO preparation and execution stages and then similar to the case of the X2 based HO, it signals the PS_S-GW for the user traffic path switch from the PS_eNodeB to the C_eNodeB.

The PS_PCRF is the key element in priority policy decisions. A rudimentary priority treatment for public safety user is provided in Appendix C.

The PS_UE's functions and procedures are the same as those set up in standard UE's [3GPP16]. The PS_UE provisioning has the public safety carrier (C1) and the commercial carrier (C2) frequencies ordered in a priority order so that the default connectivity and the initial attach is always to the dedicated public safety RAN [NPST2] [3GPP8, Sec. 5.2.4.2]. The PS_UE is populated with the operator controlled PLMN selector list which contains the preferred PLMNs in priority order [3GPP2, 3.2.2.1]. Its Home IMSI (HPLMN) is the public safety PLMN ID (highest priority). It also contains a prioritized list of permitted Visitor VPLMNs. Also, in order that the public safety user may have a nationwide coverage, it may not have any entries in the forbidden PLMN list. Also, in order to support accessibility, the USIM should be unlocked to allow a public safety user to switch out Universal Integrated Circuit Card (UICC) between multiple equipment.

5.3.2.2 Commercial Network Elements

The primary impact of this architecture for handling the public safety user is on C_eNodeB.

The C_MME, C_S-GW, C_HSS, C_P-GW, and C_PCRF are involved only in commercial user connection and traffic handling. They do not handle public safety user related interactions.

The C_MME interfaces with the C_eNodeB and directs the commercial traffic through the C_S-GW and C_P-GW in collaboration with C_PCRF.

The C_eNodeB is populated with both PS_PLMN ID and the C_PLMN ID as part of its initialization process. C_eNodeB manages the dynamic capacity value as indicated in Section 5.3.1. It restricts the commercial UE from being handed over to the PS_RAN using UE area restriction information [3GPP16, Sec. 10.4].

The commercial C_UE always connects to the commercial network and is not allowed entrance to the PS_eNodeB. Its stored Home PLMN ID could be the shared D-block PLMN ID or another commercial PLMN ID. The public safety PLMN ID needs to be on the commercial C_UE's "Forbidden PLMN ID" list so that a commercial C_UE cannot connect to the public safety network [3GPP2, 3.2.2.1]. In addition, the public safety carrier frequency (C1) is on its "blacklist" of frequencies.

6.0 Public Safety Users in the Shared Network Environment

This section builds upon the foundation set in the previous sections and applies it to the various scenarios for the public safety and the commercial user treatments in the shared network architecture under consideration. After the underlying approach and framework are discussed, several scenarios are covered.

The illustration in this section 6 of the robustness of the priority treatment for public safety users uses the architecture shown in Figure 5.1 in which the shared commercial RAN is connected to the public safety EPC via the S1 interface. Assuming the distinctness of the RANs being associated with the public safety and the commercial operators, the scenarios focus on the situation where the X2 connectivity is not deployed between the PS_eNodeBs and the shared commercial C_eNodeBs.

After the detailed treatment of the S1 based HO in this section, the X2 based HO approach is applied to the same architecture for data (ftp) type application on Section 10.3 in order to provide an alternate view of HO.

6.1 User Scenarios (Use Cases)

The underlying approach for the scenarios is indicated in the following. It may be noted that these principles are intended to be illustrative of how the priority requirements for a typical public safety user are met for the architecture indicated in Figure 5.1

1. A public safety user is initially connected to the public safety network and moves over to the shared commercial network in case of congestion in the public safety network.
2. In case of a congested public safety network, the new public safety user, regardless of its priority, does not preempt an existing lower priority user but is handed over to the shared commercial network if there is capacity in the public safety allocated region. Note that an alternate approach could be to move a lower priority public safety user to the shared commercial eNodeB instead. That may be less desirable since an existing public safety user may already have bearer established. The analysis in this study can be extended to that option as well.
3. If the commercial RAN is also congested, then the new public safety user is assigned resources in the public safety RAN by invoking the priority mechanisms by freeing up the resources from a lower priority public safety user.
4. Preemption implies, in priority order,
 - a. Reducing the bit rate to a lower value consistent with keeping the functionality at a lower CODEC rate
 - b. Handing over the lower priority user to a neighbor network
5. Only one type of application, streaming video, is considered which implies one class of "QoS" traffic bearer.
6. This study focuses on session initiation from the PS_UE. The case of a network initiated terminating session can also be treated using a similar approach based on the LTE standards for terminating sessions.

Figure 6.1 provides the overall framework for the scenarios being discussed in this section

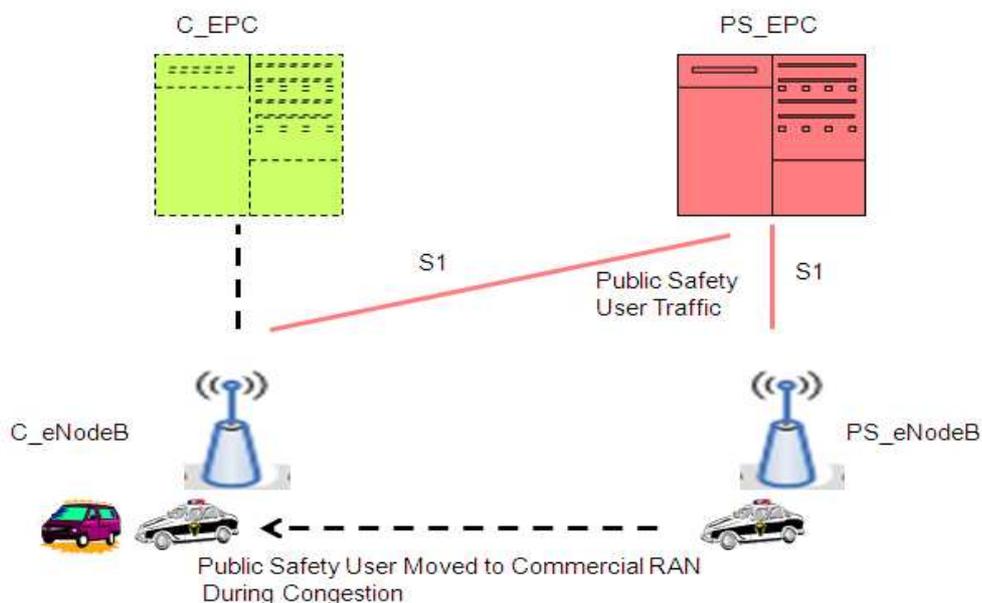


Figure 6.1: Public Safety User Handed Over to the Commercial RAN in case of Public Safety RAN Congestion

The PS_eNodeB along with the C_eNodeB are the primary entities responsible for the HO from the public safety RAN to the Commercial RAN. PS_MME is aware of the eNodeB conditions for both the public safety and the commercial RANs. For moving the public safety user from the PS_eNodeB to the C_eNodeB, the radio connection and the S1 backhaul are shifted from the public safety RAN to the commercial RAN. The commercial RAN uses the PS_EPC for public safety priority management. All commercial traffic in the shared C_eNodeB is considered at lower priority within the public safety allocated capacity domain.

In the following, the summary of the various representative scenarios are provided. The details of the scenarios are available in Appendix D.

6.2 New Public Safety User – Public Safety Network not Congested

In this basic scenario of a new public safety UE attempting to establish a bearer in the public safety network, it is assumed that the public safety RAN is not congested. This establishes the basic groundwork on how a new public safety user gets priority treatment in an unloaded system.

Figure D.1 provides the summarized view of the admission and bearer establishment for a public safety user. This is based on the Illustration of a UE initiated Service Request Procedure available in [3GPP10, Sec. 5.3.4].

Figure D.2 provides a set of detailed steps.

It may be noted that the subsequent scenario for setting up a GBR dedicated bearer is very similar to the above steps wherein the steps are initiated by the PS_UE sending a modify bearer request to the PS_eNodeB. The steps #7 onward in the above scenario are repeated and a dedicated bearer is set up.

6.3 New Public Safety User – Public Safety Network Congested, Commercial Network not Congested

This scenario pertains to the situation where the public safety user is moved over to the shared commercial C_eNodeB which has not yet reached the public safety allocated capacity limit. As indicated in Figures 5.8(a) and 5.8(b), the commercial users may or may not be in partial use of spare public safety allocated capacity. Effectively, the commercial RAN is still not congested from the public safety user perspective. The discussion here is limited only to the case of treatment for the public safety user.

The overall approach is as follows.

The new public safety user equipment attempting to get a bearer in the public safety dedicated network is directed to the shared commercial network. The PS_eNodeB and the C_eNodeB coordinate the HO from the PS_RAN which has established the initial radio communication with the target commercial RAN through PS_MME using the S1 interface. The PS_MME primarily plays the pass-through role. A normal HO scenario then results.

Such an illustrative flowchart is provided in [3GPP10, Sec. 5.3.5] and covered in Figure D.3.

6.4 Existing Public Safety User Requests Additional Resources – Public Safety Network Congested, Commercial Network not Congested

For this situation, the public safety network is congested and an existing public safety user equipment requests additional resources. One approach would be to move this requesting public safety user equipment to the shared commercial network. However, since the requesting public safety user equipment had already established a lower bit rate or a default bearer, it is preferable to move an existing lower priority public safety user to the shared commercial RAN. This involves sending both the control signaling and the traffic bearer context of the lower priority public safety user to the target commercial C_eNodeB. User traffic, if public safety user is in data transfer mode, is also switched from the public safety S1 interface to the S1 interface between the PS_MME and the C_eNodeB.

This scenario is similar to the one in Section 6.3 except that the user being moved to the shared commercial RAN will be a “lower” priority public safety user.

6.5 New Public Safety User – Public Safety Network Congested, Commercial Users Using Public Safety Capacity

This situation is very similar to the public safety perspective discussed in Section 6.3 where the public safety user is moved over to the shared commercial RAN. In that case, capacity was available in the shared commercial RAN and the commercial users had not completely used the spare capacity in the public safety allocated region. There was no impact on existing commercial users.

Now consider a situation where the commercial users have used the spare capacity and the C_eNodeB is now fully loaded as suggested in Figure 5.8(c).

If a new public safety user is handed over from the PS_eNodeB to the C_eNodeB, that public safety user needs to be given priority and an existing commercial user in the shared C_eNodeB needs to be preempted. The action on the commercial user needs to be taken by the C_eNodeB in concert with the C_MME. The C_eNodeB triggers the C_MME for preemption of the commercial user. This needs to be done prior to C_eNodeB assigning the resources to the PS_UE in the C_eNodeB (Step H in Figure D.3).

The scenario would be very similar to the one in Figure D.3 except for the intermediate step of preemption of an existing commercial user by C_MME and C_eNodeB prior to step H.

This preemption to accommodate a new public safety user may continue until the public safety users have consumed their allocated capacity in the shared commercial RAN. Then the C_eNodeB is congested from both the public safety and the commercial users’ viewpoints. Such a situation is discussed in Section 6.6.

6.6 New Public Safety User – Both the Public Safety and Shared Networks Congested

In this case, there are no resources available either in the public safety RAN or in the shared commercial RAN for the newly arrived public safety user (see Figure 5.8(d)). When the PS_eNodeB needs to send the PS_UE to the C_eNodeB, it sends the HO required message to the PS_MME [3GPP16, Sec. 19.2.2.5.1]. In this case, the PS_MME receives the HO failure message from the target C_eNodeB in response to the HO request. It sends the HO preparation failure message to PS_eNodeB. From the perspective of the C_eNodeB, congestion reflects the situation wherein the public safety users have used the public safety allocated capacity regardless of whether there is any spare capacity in the commercial allocated domain. In this situation, a commercial user cannot be preempted in the shared commercial RAN since the public safety usage in the shared commercial RAN has reached its agreed-upon allocated limit. The public safety user needs to be handled in the public safety domain and be given priority treatment within the public safety RAN and PS_EPC complex.

In order to free up resources for the new public safety user in the public safety network, the public safety RAN preempts a lower priority public safety user. An illustrative detach procedure flowchart for such a situation is available in [3GPP10, Sec. 5.3.8]. One may also refer to [3GPP10, Sec. 5.4.4] for the bearer deactivation flowchart and [3GPP16, Sec. 19.2.2.2] for context release procedure.

A representative scenario is provided in Figure D.4.

6.7 Public Safety User in Shared Network – Hand Back to Public Safety Network

As indicated in previous sections, a public safety user is handed over to the shared commercial RAN in case of congestion in the public safety network. The migration of the public safety user to the shared commercial RAN may continue until the public safety users have reached the maximum allocated capacity in the shared RAN. When the public safety UE is in the commercial RAN, the amount of resources that the commercial users can utilize is limited by the remaining spare capacity in the commercial RAN. It may be noted that in case the public safety RAN congestion decreases, then it will be prudent to move public safety user(s) to the public safety network so that the capacity in the shared RAN can be more effectively and efficiently utilized for the commercial users without compromising the needs of the public safety users. Such scenario involves handing back a public safety user along with the context to the PS_eNodeB. Note that, in general, the public safety user equipment has a dedicated bearer in the commercial RAN domain. The Hand Back (HB) scenario is not the traditional HB scenario at cell edges where the decision to move the UE back to the previous eNodeB is taken by the current serving eNodeB in case of signal strength issues. The HB in the case of the public safety user in the shared commercial RAN is triggered when the

capacity in the PS_eNodeB is freed up and it is desirable to relieve the capacity in the commercial C_eNodeB.

The scenario is initiated when resources are freed up in the public safety RAN. Since this study uses the notion of the S1 based HO without the presence of the X2 interface between the PS_eNodeB and the C_eNodeB, the trigger for moving the public safety user from the C_eNodeB to the PS_eNodeB comes from the target PS_eNodeB. The PS_eNodeB requests the C_eNodeB via PS_MME to hand over a PS_UE to the PS_eNodeB. The C_eNodeB chooses a PS_UE to be moved to the C_eNodeB. This may be based on priority levels or random selection. The PS_UE has previously continued the measurements reports with respect to the PS_eNodeB and has provided the same to its current serving eNodeB which is the commercial C_eNodeB. The standard HO process along with the bearer shift to the PS_eNodeB is then followed as indicated in Appendix D in section D.4.

6.8 Commercial User in Commercial Network

For the sake of completion, it may also be worthwhile to discuss the treatment for a commercial user in the shared commercial network. The commercial user receives normal operating treatment when it attempts to connect to the shared commercial RAN on the C2 carrier. In case there is spare capacity in the public safety allocated region, the commercial user is assigned the connection and the resources. Control and user traffic bearer for the commercial user is established between the commercial RAN and the commercial EPC as in standard commercial networks.

There are three primary situations from the commercial user viewpoint.

The first is the standard case wherein resources are available in the commercial RAN and EPC and normal connections and bearer establishment are completed. This may also occur in the spare region of the public safety allocated domain.

The second involves the case of congestion in the commercial network, i.e. no capacity either in the commercial allocated or in the public safety allocated region is available. As in standard commercial networks, the new user is blocked from the LTE network. In order to provide appropriate customer experience, this may result in fall over to the commercial carrier's LTE or 3G network or even to a 2G/2.5G network in extreme cases. In general, the commercial users are assigned the access class randomly in the priority range of 0-9. Their barring decides the radio access treatment and the ARP values determine their preempting capabilities.

Another situation arises in which the commercial users are using the spare capacity in the public safety allocated domain and the C_eNodeB is fully congested. If a public safety user is then directed from the congested public safety network (see Section 6.5), then a commercial user needs to be preempted. The choice of the commercial user to be preempted and the treatment to be provided is within the purview of the commercial C_eNodeB and C_MME. The action may involve moving or handing over the commercial user to another network as stated above.

7.0 Rules of Engagement / Agreements between Public Safety and Commercial Organizations

The approach of using a dedicated public safety network with a shared commercial network provides an excellent framework for a cooperative relationship, revenue generation, and leveraging of the commercial expertise and services for the benefit of the nationwide public safety solution. This requires agreement on rules of engagement which may be implemented in the form of NSA. Framework for such agreement has also been provided previously in [NPST2], [PSST1], [MANN]. The recommendations in this section should not be construed as commitments by the public safety or the commercial partner but are intended as working principles which may form the basis of an NSA.

In general, most of these rules of engagement are not restricted to the dedicated public safety and the shared commercial network alternative discussed in this study, but would also apply to any other alternative which involves (especially in emergency situations) HO or roaming to another LTE (or other technology) networks. For the shared network architecture chosen in this study, NSA is considerably simplified since the interactions between the two network entities are minimal and well-defined, as compared to other options.

The key elements of the NSA are summarized in the following.

In order for the public safety user to be able to utilize the shared RAN resources, while at the same time the commercial users can utilize any spare scarce resource in the commercial network, the primary agreement needs to be on the value of the PS_max_capacity limit indicating the allocated public safety capacity in commercial RAN. It may be noted that in extenuating circumstances, the commercial organization may need to provide all the resources for the public safety users to be consistent with the national interest. Hence, the agreement needs to be established on a simple and fast process by which the public safety organization can intimate the commercial operator to raise the limit value to a higher desired value. It is expected that the request for modification of the limit value will be honored by the commercial partner as part of the NSA agreement. Commercial C_eNodeB and PS_MME also need to cooperate so that they can manage the public safety user while in the shared C_eNodeB within the allocated public safety capacity.

This study has shown that public safety user's priority treatment and management in the shared commercial domain can be the same (or similar) as in the dedicated public safety network domain. This may require agreements on parameters, attributes, and their application for public safety and commercial users, e.g., HO associated measurements [3GPP16, Sec. 11.3], UE/eNodeB synchronization methods [3GPP16, Sec. 4.4], IP fragmentation strategies [3GPP16, Sec. 4.5], and security aspects among others. This may also need to include the scheduler algorithms and rate control procedures for providing per-packet based treatment [3GPP16, Sec. 11] to allow the same bearer handling treatment in both networks. Scheduling algorithms are not standardized and are eNodeB vendor specific, see e.g., [MONG]. These may include round robin scheduler, proportional-fair scheduler, and max C/I scheduler. It is also expected that eNodeBs shall provide public safety users higher priorities in situations requiring queuing for resource allocation. Strategies of

reserving some resources due to the statistical nature of the user and traffic scenarios need to be agreed on.

Agreements need to be established for priority parameters, e.g., traffic class priority, ARP priorities, ARP preemption and vulnerability. The transfer of information between the two RANs especially for HO needs to be agreed upon. The use of high priority access-oriented preamble and establishment cause parameters need to be provided by the C_eNodeB to the PS_UE. Similarly for HO priorities, when a visitor comes to a network, the visitor is generally treated at a lower priority than a user from the home network. This needs to be altered to allow the public safety user higher priority during HO. Consistent security mechanisms among the networks and for UE treatments need to be agreed upon.

Inter Operator Testing (IOT) is another area of agreement that needs to be in place. The networks should be able to successfully interface with each other and it is expected that the vendor implementations should allow such consistent interfaces. This is quite similar to standard commercial network environment involving HO and roaming requirements.

Note that such agreements are needed not only for the dedicated public safety and shared commercial architectures discussed in this study, but also for all other alternatives wherein HO/roaming is expected to a commercial LTE (or other technology) alternatives.

For the respective user equipment, the provisioning, capabilities, and restrictions of the UEs should be consistent with the strategies for this architecture. The PS_UE needs to be populated with both the public safety carrier (C1) and the commercial Carrier (C2) with C1 as the higher priority order. Its highest priority and home PLMN ID will be the public safety network PLMN ID.

In this example, the commercial UE will be provisioned with only the commercial C2 frequency. The public safety frequency will be put on its “blacklist” so that it does not connect to, be handed over to, or roam into the dedicated public safety network.

The shared C_eNodeB and the S1 interface between the C_eNodeB and the PS_EPC are shared resources between the two entities. Agreements need to be established on the ownership, engineering, deployment, maintenance, and management of the shared S1 connectivity.

The state of the C_eNodeB and the S1 interface between the C_eNodeB and PS_MME is of particular significance to the public safety agency. The fault conditions, recovery actions, and release update situations need to be conveyed to the public safety agency. The Network Management System (NMS) and Operations Support System (OSS) need to support such notifications. Also, the public safety user, while in the shared C_eNodeB, would expect customer support in case of C_eNodeB failure conditions. That support may continue to be provided to the public safety user by the public safety customer support team which is dependent upon timely and accurate state information from the commercial operator. The public safety user expects consistent and effective customer management support regardless of whether he or she is in the dedicated public safety RAN or the shared commercial RAN.

It is expected that there will be appropriate revenue transfer agreements between the two organizations primarily reflecting the usage of the shared commercial resources by the public safety user.

Related to this approach of shared networks is the standard roaming agreements between the commercial operators and public safety provider as part of providing nationwide coverage for the public safety users, e.g., acceptance of a public safety IMSI for service [3GPP2, 2.1]. This is of particular significance during the foreseeable future when the public safety network will be in its build-up phase.

Such a sharing approach creates a mutually beneficial relationship between the public safety and the commercial organization, and creates several opportunities for cooperative deployments, economy of scale, and common approach for services and applications. This includes developing mechanisms for future requirements and evolution [NPST2] and a common advocacy to the standards bodies for new and required features and capabilities.

Finally, the public safety community should develop a common and uniform management framework for the nationwide public safety network, balancing regional and local control. A common set of requirements needs to be in place with a common set of priority mappings for all public safety agencies. This may also require a common representative body (or bodies) for setting requirements, establishing agreements, and managing the nationwide public safety network.

8.0 Additional Support from LTE Standards for Handling Public Safety Priority Management

LTE/EPC Release 8 and the subsequent Releases 9 and 10 provide a very strong foundation and framework for meeting the priority management needs of the public safety users, both in the dedicated public safety network as well as in the shared commercial network. However, there are areas in which additional standards development may be desirable to meet the enhanced and future needs of the public safety community. This section highlights some of these areas. Several areas have also been previously identified as issues in [MOTO1]. The focus in this study is on the methods to address the relevant issues for the architectures described in this study. These issues do not impede the implementation of priority access for shared networks under the current set of standards.

Six access classes for emergency and other operations for the public safety community have been proposed in this study: one for emergency situations for all public safety personnel and five for non-emergency situations for the five groups of public safety communities. In the current LTE standard, three (12–14) are available for the public safety community. Availability of three additional dedicated-access class priority levels is proposed for exploration by the 3GPP standards body. This would bring the total to 6 levels.

It is also desirable to have an “Inactivity Timer” to handle the situation where the network could have the option of bringing down a GBR bearer if the public safety user has not used it for a period of time (inactivity time). In order to allow the emergency public safety user and the executive public safety user to keep their GBR bearer even if they have been dormant for some time, this flag may be set to “no” for the highest two classes and “yes” for the others. This is to avoid the emergency public safety and executive PS5 users having to set up GBR bearers again.

Broadband requirements for the public safety users are expected to be more stringent than commercial users. This may involve different priority treatment that is customized towards specific applications, e.g., dropping a video session and keeping a voice session in case of restricted availability of resources.

Also, the public safety community could re-evaluate the requirement that at least 50% or a minimum of 8 ARP priority levels be available for public safety usage (out of 15). This study proposes that six levels could be sufficient for public safety use out of the 15 available.

9.0 Other Illustrative Shared Network Architectures

In Section 5, three major architectures were presented. The architecture shown in Figure 5.1 was used as a basis for illustrating how public safety priority requirements can be met in the dedicated public safety and shared commercial network solution. Using the detailed treatment given to the architecture addressed in the previous sections as the foundation, the corresponding discussion is provided in sections 9.1 and 9.2 for the other two architectures of Figure 5.2 and 5.3 respectively.

9.1 Shared RAN Architecture

The public safety priority management analysis for the shared RAN architecture is very similar to the one discussed using the interconnection of the C_eNodeB with the PS_EPC. There is a PS_max_capacity limit in each eNodeB to indicate the maximum allocated capacity for the public safety user in which the public safety user will always get the priority treatment with respect to the commercial user. The major scenarios and operational summary are provided in Appendix E.1.

9.2 Independent Public Safety and Commercial Network Architecture

In this section, the priority study previously applied to the architectures of Figure 5.1 and 5.2 is extended to the architectural option of the public safety and the commercial RANs being connected to their respective EPCs (see Figure 5.3). This implies that, in case of congestion in the public safety network, the public safety user will be handed over to the co-located commercial network. For the HO, inter-frequency HO will still be required. The public safety traffic while in the commercial RAN can be directed through the PS_P-GW (Home Routed) or through the commercial C_P-GW (Local Breakout) similar to the situations in a roaming scenario. The Home Routed is preferred since the public safety priority treatment is then managed by the PS_PCRF. The summary of the application of public safety priorities for this alternative is provided in Appendix E.2.

10.0 Applicability and Extensions of this Study

This study has focused on representative details of three architectures indicated in Section 5.1. Use has been made of streaming video as a representative example. The basic 3GPP mechanisms which support the public safety user for ensuring their priority treatment have been identified. The public safety user gets consistent priority treatment whether in the dedicated public safety network or in the shared commercial network.

This study can be extended to other situations of interest to the public safety community.

The public safety dedicated network is generally expected to have spare capacity which can be utilized effectively by second responders and local, regional, or federal employees.

It is also expected that for a considerable amount of time during which the national public safety network is being built, the public safety users will request access to commercial LTE networks operating in the 700 MHz region.

Although streaming video is likely to be a major initial application, the data and other video services will be critical for the public safety community.

Security and the access to home zone services are very critical for the public safety community regardless of where they are roaming at any time. The notion of Public Safety Private Data Network (PSPDN) is a major requirement from the public safety community's viewpoint.

In this study, restrictions were placed on the commercial users; they are not allowed in the dedicated public safety network. If this restriction is lifted, then the commercial users can be handed over to the public safety RAN and their traffic can be sent through the commercial EPC without compromising public safety priority requirements. This will result in much better use of the scarce spectrum resource.

Finally, the LTE standards are expected to evolve. The Release 9 and Release 10 specifications are already in place and they provide several advanced features of direct relevance to the public safety community.

In the following, the discussion and results for these extensions and applicability are presented.

10.1 Extended Public Service and Federal Community

The focus of this study has been primarily on the public safety first responders. This community includes police, firefighters, and emergency medical personnel. During an emergency, there are volunteers and backup persons who support the first responders. In addition, as long as the priority treatment for the first responders is not compromised, other local, state, and federal personnel may be supported on the dedicated public safety network. This would allow very effective use of the scarce spectrum resource in the national interest.

A basic approach for handling these two sets of communities could be to treat them at a lower priority as is done for commercial users. Similar to the approach of managing the commercial users in the commercial networks, the randomly assigned access priorities 0–9 can be used for these Other Public (OP) services persons and assignment of priority 10 for emergency use. Similarly, the ARP treatment will be consistent if the OP users are considered equivalent to the commercial users.

A summary for the radio admission control and ARP attributes for OP users and their relationship to the attributes for the public safety users is provided in Tables 10.1 and 10.2. These are similar to Tables 3.4 and 3.5 since the OP users are treated the same as commercial users in a shared environment.

Table 10.1: Public Safety and Other Public (OP) Persons – Radio Admission Control

User Priority	User Identification	Traffic Class	Barring (RACH)	Establishment Cause (RRC)
PS First Responders	PS Emergency to PS5	12 - 14	BarringForSpecial	HighPriorityAccess
OP User Emergency	OP User Emergency	10	BarringForEmergency	Emergency
OP User Non-Emergency	OP User Non-Emergency	0 - 9	Low BarringFactor	Mobile Originating

Table 10.2: Public Safety and Other Public (OP) Persons – Allocation and Retention Priority (ARP)

User Priority	APR Priority (1 highest)	Preempt Others	Preempt Vulnerability
PS First Responders	2 - 7	YES	YES/NO
OP User Emergency	8	YES	NO
OP User Non-Emergency	9 - 15	NO	YES

It is proposed that, in case of congestion in the public safety network, the public safety network will not automatically move these OP users to the shared commercial network as is done for the first responders. Also, they will not be considered as part of the allocated public safety capacity in the shared commercial network.

These additional users may be treated for access to the commercial network similar to the normal HO and roaming scenarios in the commercial networks where proper NSAs exist. This implies that after HO to the shared commercial RAN, the OP users will be considered as part of the commercial domain and compete with other commercial users for resources. The preferred approach in commercial networks for ARP treatment for mobile users being handed over from another network or roaming into a network is to assign lower priority than the subscriber in their home network. This is done by allocating the visiting user lower ARP priority as compared to the home commercial user. Similar attribute assignment can be applied for second responders and federal personnel in the commercial networks.

When the OP user moves to the shared commercial network, the OP traffic will not propagate through the S1 connection between the C_eNodeB and the PS_EPC. Instead, either of the two approaches — Home Routed or Local Breakout — can be taken for the OP user traffic.

10.2 Other Network Connections for Public Safety Users

Due to the slow build-out of the 700 MHz public safety network, the public safety user is expected to connect to other networks in the foreseeable future from both roaming (nomadic access) and HO perspectives.

The proposed priority order for HO and roaming for public safety users in the 700 MHz band is indicated below [NPST2].

1. HO between and roaming into 700 MHz public safety LTE networks
2. HO between 700 MHz public safety LTE and commercial partner shared LTE network(s) as well as roaming into these networks

This implies that the public safety user needs to be able to roam into 700 MHz frequency band networks. The Home PLMN (HPLMN) has the capability to steer a public safety user to specific and preferred Visitor PLMN (VPLMN), e.g., another public safety network instead of a commercial network [3GPP2, Sec. 3.2.2.8]. The radio access treatment for a public safety user can also be provided in a visitor network [3GPP2, Sec. 4.3].

It may be noted that HO and roaming into other partner 3GPP or non-3GPP networks is also expected by the public safety community, especially in regions where 700 MHz LTE networks do not exist. Both HO mobility [3GPP16, Sec. 10.2.2] and roaming into the WCDMA/HSPA [3GPP16, Sec. 10.2] and the CDMA2000 [3GPP16, Sec.10.3] networks can be supported. The Inter-RAT measurements to enable such HOs [3GPP10, Sec. 5.5.2], [3GPP17, Sec. 5.4] are defined [3GPP16, Sec. 10.2.3], [3GPP17, Sec. 5.5]. The flowcharts and details for Inter-RAT HO are provided in [3GPP10, Sec. 5.5.2]. A very efficient approach for packet Inter-RAT handover is also covered in [3GPP10, Sec. 5.6] on network assisted HO. It may be noted that roaming onto 3G technologies, such as CDMA2000 and WCDMA/HSPA, might not provide support for the same prioritization scheme as envisioned for LTE networks. However, NSAs and appropriate roaming protocols could define how such roaming would be handled on a prioritization basis.

The priority treatment for the public safety user while roaming into a visitor 700 MHz LTE network is implemented via the rules derived from the public safety home network. The visitor core network interfaces with the home PS_PCRF to provide the priority treatment to the visiting public safety user. The analysis in this study for public safety priority treatment can be extended to these scenarios.

The core commercial network operator needs to pre-define their relative share of visiting roamers and distribute the visiting roamers and apply automatic network selection to different core networks connected to the radio access network accordingly [3GPP2, Sec. 2.4].

Some representative examples and how they will be handled are mentioned in the following.

Consider the situation when the public safety RAN is down and only the shared commercial network is available. The public safety EPC may still be operational and be able to support the public safety traffic. This situation is basically a roaming scenario from the PS_UE perspective and the commercial RAN/EPC complex works with PS_HSS and PS_PCRF to provide the priority treatment for the public safety user.

Another scenario may involve the public safety user roaming into another dedicated public safety network. Since the visited public safety network and the home public safety networks are at the same frequency, the PS_UE operates at the same public safety assigned frequency. The type of HO to

another public safety network including the home public safety network would be an intra-frequency HO supported by intra-frequency measurements [3GPP16, Sec. 10.1.3.1].

As part of the standard roaming scenarios, there are two options as mentioned previously. These are summarized in Appendix F.

To support roaming into commercial D-Block and other 700 MHz (and other bands) LTE networks, multi band frequency (including band 14) enabled UEs, are expected to be available early 2011 [PSCR2.]

For roaming into other 3G networks, the UE's need to be dual/multimode units [3GPP2, Sec. 3.2.3] and these are expected to become available in the next 1–2 years [PSCR2].

10.3 Handling of a Data (ftp) Application

The application studied in this document has been the streaming video application. The public safety environment is one which requires the quadruple play multimedia services including audio, video, data, and mobility. The LTE Release 8 supports the multimedia application via the QCI mapping and also sets the foundation for multimedia support based on the IP Multimedia System (IMS) based Multimedia Priority Service (MPS) [3GPP3] architecture. This section addresses the treatment for a data (ftp) type application and shows how it can be supported in the dedicated and shared commercial architecture (Figure 5.1). In the LTE priority structure, the streaming application is assigned the QCI bearer 4(GBR Table A.3) which is handled at scheduling priority level 5 (1 being the highest). The packet error rate requirements for such an application are not stringent and hence during HO to another network, some discontinuity in user traffic during HO may be acceptable.

A typical data application may involve ftp, www, and email type services which do not have stringent real time latency requirements but do require very tight packet loss requirements. In LTE, data applications can be assigned three QCI values 6, 8, or 9 with each of the associated bearers being non-GBR. The corresponding packet treatment priority levels are the lowest 6, 8, and 9 respectively. In the standalone public safety network, the data application undergoes similar treatment as the streaming video application considered previously. However, during an HO scenario, the treatment for the data application needs to be quite different as compared to the streaming video application. The handling of the data application entails continuity of user traffic during HO. The approach for such an HO scenario using the X2 based interface is provided in Appendix G.

10.4 Public Safety Private Data Network (PSPDN)

One of the public safety community requirements is for the regional operator and commercial networks operating in conjunction with the public safety agency to allow establishment and use of secure Virtual Private Network (VPN) connections for public safety users while roaming into visitor networks [NPST2]. This can, potentially, be achieved by implementing an overlay network on the

Public Data Network (PDN) to provide a Virtual Private Network (VPN) to the public safety community. This is to ensure that a public safety user receives end-to-end priority treatment and security functionality that is the same as in home public safety network. In this study, the focus has been on the priority management in the LTE/EPC access and core entities. The treatment needs to be extended end-to-end using the IETF protocol like DiffServ / IntServ and IPSec [IETF].

10.5 Allowing Commercial Users into the Public Safety Network

One of the recommendations in [NPST2] is that public safety users that are part of a regional system may roam off of the national system and *commercial users may roam onto the national system*. The public safety users still need to be guaranteed the expected priority treatments. This allows use of the “spare” capacity in the public safety network to be efficiently used and creates additional revenues for the public safety community. In other words, the total capacity of both the public safety RAN and the commercial RAN is fully utilized by this logical merging of the public safety and the commercial users in both RANs. Also, the approach allows economy of scale so that the public safety community will have less expensive UEs.

The architecture and priority mechanisms studied in this document can support such use of the public safety network by the commercial users without compromising the public safety priority requirements. In the basic architecture of Figure 5.1, for example, the separation of the public safety and the commercial traffic can still be maintained by using a new S1 interface between the PS_eNodeB and the C_EPC as a mirror image of the case where the public safety user traffic from the C_eNodeB is transported over the S1 connection between the C_eNodeB and the PS_EPC (see figure 10.1). This also becomes somewhat similar to the shared RAN approach.

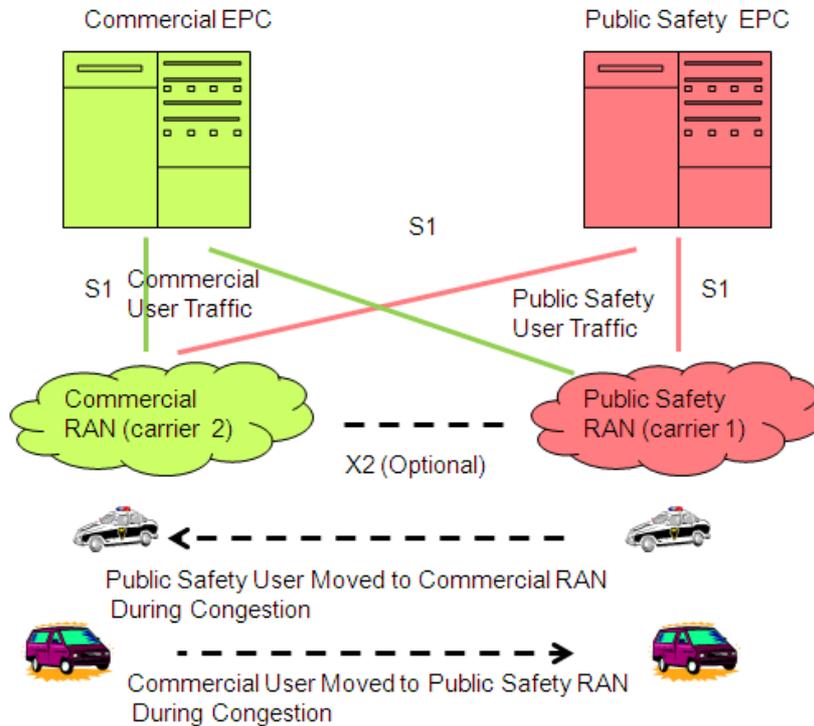


Figure 10.1: Commercial User Allowed in Public Safety RAN; Commercial traffic through C_EPC

Consistent priority treatments need to be applied and attributes need to be populated for the public safety user and the commercial users in the corresponding PS_HSS and the C_HSS respectively. Coordination is required between the PS_eNodeB and the C_eNodeB to support load management between the two eNodeBs. As with the PS_UE discussed previously, dual (multi) frequency UEs are also needed for the commercial users.

The basic priority management scenarios for the commercial users would be very similar to the case of Other Public (OP) user treatment discussed in Section 10.1. The priority treatment for the public safety community is not compromised.

10.6 LTE/EPC Evolution

Choice of LTE/EPC technology will allow the public safety community to benefit from the 3GPP standards evolutionary path and the related functionalities and capabilities which will be introduced. Some of the known facilities for the benefit of the public safety community are summarized in this section.

10.6.1 LTE Releases

In this study, Release 8 was used because it introduces the basic priority mechanisms needed to meet the public safety community's requirements. Release 8 introduces advanced air interface, all Internet Protocol (IP) treatment, priority structure, QoS, and superior performance. In the

following, some of the LTE capabilities in subsequent releases which could be of interest to the public safety users are mentioned.

LTE Release 9 includes Multiple Input Multiple Output (MIMO) enhancements, Software Defined Radio (SDR), Self Organizing Network (SON), Multimedia Broadcast / Multicast Service (MBMS), Personal Area Networks (PANs), and security enhancements. The SDR capabilities allow Software Upgrades (SUs) in a smooth manner in addition to assists in choosing appropriate frequency of operation and synchronization. SON allows configuration data to be shared between the various eNodeBs and enable fast recovery actions in case of failures.

Related Closed Service Group (CSG) capabilities provide localized group calling capabilities which are of considerable interest to the public safety community. The CSG capability is supported via Home H-eNodeBs [3GPP2, Sec. 8], [3GPP16, Sec. 4.6], [3GPP5]. This was introduced in Release 8 and requirements have been consolidated in Release 9.

The features of interest to the public safety community in LTE Release 10 include relay nodes, emergency call treatment, UE dual TX options, flexible spectrum usage, cognitive radio, and automatic network configuration.

While the actual process of coordinating LTE releases to public safety and commercial networks is considered beyond the scope of this study, it is important to develop a roadmap for priority access evolution so that consistency with future LTE releases is maintained, and enhancements contained in future releases are used to advantage.

10.6.2 IP Multimedia Service (IMS) and Multimedia Priority Service (MPS)

IP Multimedia Service (IMS) is a service architecture for handling multimedia applications. The architecture allows the provisioning of application servers for video, audio, and data services. This will likely also become the commercially accepted approach for providing voice services. Voice over LTE (VoLTE), a feature of critical interest to the public safety users, with suitable adaptation to public safety requirements, may allow migration from the existing LMR type systems to a broadband network. Multimedia Priority Service (MPS) allows considerable flexibility in assigning user priority levels [3GPP3, Sec 5.5]. Also, the Next Generation GETS (NGN/GETS) initiative relies on the longer range architecture based on IMS [NCS].

10.7 Items for Further Discussion

This study focused on a UE originating session scenario as a framework. It can be extended to analyze a mobile terminating session scenario (incoming). For such network origination cases, the P-GW is the primary unit (like the UE in the originating case) which requests for initiation of the incoming session to the UE. P-GW may undertake Deep Packet Inspection (DPI) to define and identify the Service Data Flow (SDF) characteristics. The interface with the UE involves paging permission with access control [3GPP4], [3GPP11, Sec. 5.6.2]. Connection and bearer may be established with the UE even if terminating side is in congestion. Paging and control plane establishment is covered in [3GPP16, Sec. 10.1.4]. Discussion on cases where the (network)

originating or the terminating UE is a public safety priority user or another non-priority user is available and the issues relating to the terminating UE not being a priority user are mentioned [3GPP4, Secs. 4, 5].

An extension would be the discussion on session termination [3GPP16]. The scenario will involve tearing down the bearer, freeing up the resources, and generating charging records.

Another area for extension is studying and identifying the interactions of the priority mechanisms with other advanced features. Generally, no interactions are expected between the priority service and other supplementary services [3GPP6, Sec. 5.5]. In case the public safety community needs specific types of relationships between the priority management features and other features, then recommendations may need to be provided to the 3GPP standards body.

11.0 Conclusion

Priority mechanisms based on the capabilities of the LTE/EPC family of standards can meet public safety requirements and provide emergency communications capacity on commercial D-Block and other LTE networks in the 700 MHz band, in addition to the capacity provided by the dedicated broadband public safety spectrum. There have been various requirements efforts and proposals for public safety user requirements and for providing an architectural framework [SAFE] for a public safety nationwide network. This study has taken a core set of requirements and mappings and applied the LTE/EPC mechanisms for public safety users in the context of a dedicated public safety network interworking with a shared commercial network.

Typical wireless network architectures address standard HO from one base site to another at cell coverage boundaries. In contrast, this study has addressed HO due to congestion in the dedicated public safety network as well as Hand Back (HB) when resources dynamically are freed up in the dedicated public safety network. Some of the distinctive features of this study are: capacity-based HO, HB to the public safety network, specific distinctive architectures, reserved resource allocation for public safety users in the shared commercial network while at the same time guaranteeing resources for commercial users, use of multiple access classes and priorities, and full use of the 3GPP ARP priority mechanisms.

These mechanisms and architectures demonstrate the feasibility of the FCC's National Broadband Plan (NBP) recommendation to license the 700 MHz D-Block for commercial use and encourage incentive-based partnerships between commercial 700 MHz licensees and public safety. Recognizing that the capacity limits of any broadband public safety network can be exceeded in emergency situations, the approaches to provide additional overflow capacity for public safety described here are applicable not only to sharing of bandwidth on commercial D-Block networks, but also to the use of other broadband commercial networks in the 700 MHz region. The key support for public safety users and how they get priority treatment is summarized in Table 11.1.

Table 11.1: Public Safety User Priority with respect to Commercial Users

Driver	Mechanism	Comment
Radio Access	<ul style="list-style-type: none"> •Sufficient Control Channels •Admission Barring for Commercial Users 	<ul style="list-style-type: none"> •RACH Engineering •Barring for Special for PS Users
Radio Resource Control	<ul style="list-style-type: none"> •Establishment Cause 	<ul style="list-style-type: none"> •High Priority Access for PS Users
Traffic Bearer	<ul style="list-style-type: none"> •ARP Priority •Preempt Others •Preempt Vulnerability 	<ul style="list-style-type: none"> •Higher for PS Users •Yes for PS Users; Not for Commercial Users •Yes/No for PS Users; Yes for Commercial Users

In general, priority treatment for a public safety user applies during the following procedures:

- Resource allocation during call / session processing.
- Transport and processing of signaling messages.
- Transport and processing and transport of the traffic bearer packets.

Any congestion on the radio resources for UE-initiated access is handled using the access class barring mechanism. Congestion for admission of dedicated bearer resources is handled by applying appropriate ARP.

As suggested in the study, the preemption of a lower priority user may involve the following actions in the precedence indicated.

- Operate at lower performance, e.g., reduce CODEC rate
- Hand over to another neighbor network

The application of the above mentioned priority access mechanisms for a public safety user, in particular, in commercial and other public safety networks, is summarized in Table 11.2.

Table 11.2: Priority Access in Networks – Public Safety and Commercial

Public Safety Requirement	Priority Access Solution
Ubiquitous, Interoperable Coverage (Wherever 700 MHz Service Exists)	<ul style="list-style-type: none"> •Home Access Where Both Dedicated Public Safety and Shared Commercial Networks Exist •Roaming Access on Commercial Network if No Dedicated Public Safety Network Exists
Public Safety Users Get Through on a Crowded Control (Access) Channel	•LTE Inhibits Transmission from Commercial Users (LTE Access Barring)
Public Safety Traffic Gets Through on a Crowded Traffic Channel	•LTE Can Preempt Commercial Traffic If Necessary to Allow Public Safety Traffic Through (LTE Allocation Retention Priority)
Public Safety Has Guaranteed Broadband Capacity on the Shared Commercial Network	<ul style="list-style-type: none"> •Pre-Set (extendable), Guaranteed Public Safety Capacity on Shared Commercial Network Through Agreement with Commercial Carrier •Adds to Capacity on Top of Exclusive Public Safety Dedicated Spectrum
Automatic Access to the Shared Commercial Network	•Automatic LTE Handover to Shared Commercial Network Where Both Dedicated and Commercial Networks Exist

The adoption of the LTE standard by both the public safety and commercial operators for network deployment in the 700 MHz band provides a unique opportunity for the public safety community. The priority mechanisms that are part of the LTE standard are ideally suited for meeting public safety’s operational need to provide both hierarchical and situational priority access, and the LTE architecture is readily configured to provide the necessary functionality. LTE’s radio admission control function guarantees public safety user access to dedicated public safety and shared commercial LTE networks, even in network congestion situations, and the assignment of priority classes to public safety data traffic after initial network access ensures that public safety traffic is serviced according to the pre-determined priority structure. LTE’s ARP mechanism allows higher priority public safety user traffic to preempt lower-priority commercial user traffic.

Deploying a 700 MHz commercial network in a shared manner with the public safety dedicated broadband network using the priority approach described here provides significant advantages for public safety users beyond the availability of additional bandwidth in emergency situations.

- Deploying the dedicated public safety network using cell sites and radio access equipment shared with commercial operators allows the public safety community to leverage the high-density cell site commercial infrastructure and achieve significantly higher capacity on its

own dedicated spectrum than would be achieved with an independent, low-density cell site deployment, at the same level of capital expenditure.

- Because commercial 700 MHz networks will be built out much more rapidly than public safety networks, and over larger, nationwide coverage footprints, public safety users will gain access to advanced 700 MHz broadband services much more rapidly and over a larger area than they would with multiple, independent public safety network regional build-outs.
- Public safety entities will have access to capacity on commercial networks, particularly in rural areas, where dedicated public safety networks are unlikely to be deployed.
- With a shared commercial network, not only will the public safety community be able to use commercial capacity when emergency needs dictate, but public safety network will have the ability to permit commercial users to utilize any unused capacity on the dedicated public safety spectrum, providing for more efficient spectrum use overall, as well as public safety with a revenue source to fund its operation of a broadband network.
- The substantially larger user equipment volumes generated by devices and components which span both dedicated public safety and commercial spectrum will generate significantly lower equipment costs to public safety users than would an independent public safety network build-out.
- Large, multi-cell broadband networks, such as will be deployed at 700 MHz, are significantly more complex than current public safety networks, and a shared public safety and commercial network build-out using the dedicated public safety spectrum and commercial D-Block spectrum will allow the commercial operator's deployment, and operations, administration, and maintenance experience to be leveraged to advantage by public safety.

References

- [3GPP1] 3GPP Partnership Project, *Vocabulary for 3GPP Specifications*, TR 21 905
- [3GPP2] 3GPP Partnership Project, *Service Accessibility*, TS 22 011 890
- [3GPP3] 3GPP Partnership Project, *Multimedia Priority Service*, TS 22 153 820
- [3GPP4] 3GPP Partnership Project, *Study on Paging Permission with Access Control*, TR 22 908 810
- [3GPP5] 3GPP Partnership Project, *Service Requirements for Home H-NodeB and Home H-eNodeB*, TS 22 220 950
- [3GPP6] 3GPP Partnership Project, *Priority service feasibility study*, TR 22 950 800
- [3GPP7] 3GPP Partnership Project, *User Equipment (UE) radio transmission and reception*, TS 36 101 8b0
- [3GPP8] 3GPP Partnership Project, *UE Procedures in Idle Mode*, TS 36 304 890
- [3GPP9] 3GPP Partnership Project, *Policy and charging control architecture*, TS 123 203 8b0
- [3GPP10] 3GPP Partnership Project, *Technical Specification Group Services and System Aspects; GPRS enhancements for E-UTRAN access*, TS 23 401 8c0
- [3GPP11] 3GPP Partnership Project, *Non Access Stratum (NAS) Protocol for Evolved Packet System (EPS)*, TS 24 301 870
- [3GPP12] 3GPP Partnership Project, *Policy and Charging Control Over Gx Reference Point*, TS 29 212 890
- [3GPP13] 3GPP Partnership Project, *Policy and Charging Control Signaling Flows and Quality of Service (QoS) Parameter Mapping*, TS 29 213 891

- [3GPP14] 3GPP Partnership Project, *Evolved Packet System (EPS), Mobility Management System (MME), and Serving GPRS Support Node (SGSN) Related Interfaces Based on Diameter Protocol*, TS 29 272 880
- [3GPP15] 3GPP Partnership Project, *3GPP System Architecture Evolution (SAE); Security architecture*, TS 33 401 870
- [3GPP16] 3GPP Partnership Project, *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN), Overall description*, TS 136 300 8c0
- [3GPP17] 3GPP Partnership Project, *Radio Resource Control: Protocol Specifications*, TS 36 331 8c0
- [ALU1] Alcatel-Lucent White Paper, *Ultimate Wireless Broadband Solution for Public Safety*, 2010. http://enterprise.alcatel-lucent.com/private/active_docs/RMK7526100309_Public_Safety_EN_StraWhitePaper.pdf
- [ALU2] Alcatel-Lucent White Paper, *A How-To Guide for LTE in Public Safety*, 2010. <http://enterprise.alcatel-lucent.com/?dept=ResourceLibrary&page=WhitePapers>
- [ALU3] Alcatel-Lucent White Paper, *Introduction to Evolved Packet Core*, 2009. http://www-lte.alcatel-lucent.com/locale/en_us/downloads/wp_mobile_core_technical_innovation.pdf
- [BAJZ] Bajzik, K, Horváth, P, K_Rössy, L, and Vulkán C, *Impact of Intra-LTE Handover with Forwarding*, Mobile and Wireless Communications Summit, 2007. ieeexplore.ieee.org/iel5/4299028/4299029/04299274.pdf
- [BROU] Brouwer, W, *QoS in LTE*, Presented at PSCR2, Dec 2, 2010. http://www.pscr.gov/projects/broadband/700mhz_demo_net/stakeholder_mtg_122010/day_1/5.2_qos_priority_preemption-alu.pdf
- [CALD] Caldwell, A and McEwen, H, *Building a Nationwide Public Safety Broadband Network*, Apr 28, 2008. www.nfpa.org/assets/files/PDF/Member%20Sections/Caldwell.ppt
- [FCC1] Federal Communications Commission, *Connecting America: The National Broadband Plan*, 2009. <http://www.broadband.gov>
- [FCC2] FCC White Paper, *The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance, and Cost*, June 2010. <http://fcc.gov/pshs/docs/releases/DOC-298799A1.pdf>
- [FCC3] FCC Second Report and Order, *In the Matter of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communication Requirements Through the Year 2010: Establishment of Rules and Requirements for Priority Access Service*, Released July 13, 2000. <http://wps.ncs.gov/documents/242.pdf>
- [HALL] Hallahan, R and Peha, J, *Policies for Public Safety Use of Commercial Wireless Networks*, 38th Telecommunications Policy Research Conference, Oct. 2010. http://tprcweb.com/images/stories/2010%20papers/RHallahan_JPeha_TPRC2010.pdf
- [LIND] Lindstrom, M, Ericsson, *LTE-Advanced Radio Layer 2 and RRC aspects*, 3GPP LTE-Advanced Evaluation Workshop, Dec. 2009. http://www.3gpp.org/ftp/workshop/2009-12-17_ITU-R_IMT-Adv_eval/docs/pdf/REV-090004_Radio_layer_2_and_RRC_aspects.pdf
- [MANN] Manner, J, Newman, S, and Peha, J, *The FCC Plan for a Public Safety Broadband Wireless Network*, 2010 Telecommunications Research Conference. www.tprcweb.com/images/stories/2010%20papers/Peha_2010.pdf
- [MILL] Miller, L, *Wireless Technologies and the SAFECOM SoR for Public Safety Communications*, 2005. www.nist.gov/itl/antd/upload/WirelessAndSoR060206.pdf
- [MONG] Mongha, G., Pedersen, K.I., Kovacs, I.Z., and Mogensen, P.E., *QoS Oriented Time and Frequency Domain Packet Schedulers for the UTRAN Long Term Evolution*, Proc. IEEE Veh. Technology Conference, May 2008. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=04526113

- [MOTO1] Motorola Submission to FCC, *Public Safety Capacity Requirements Analysis*, Apr 12, 2010. <http://ecfsdocs.fcc.gov/filings/2010/04/12/6015555014.html>
- [MOTO2] Motorola White Paper, *THE BEGINNING OF THE FUTURE: 4G PUBLIC SAFETY COMMUNICATIONS SYSTEMS*, Sep 2010. http://www.motorola.com/web/Business/US-EN/NGPS/pdf/4G_LTE_Public_Safety_Communications_Systems_White_Paper.pdf
- [NCS] National Communications System, *NGN Services Priority Efforts*, Mar 22, 2010
- [NFPS] National Forum on Public Safety Broadband Needs, *Operational Requirements for the National Public Safety Broadband Network*, Aug 23, 2010. www.npstc.org/documents/ForumOnPSBroadbandNeeds100819.pdf
- [NEWM] Newman, S and Peha, J, *The Public Safety Broadband Wireless Network: 21st Century Communications for First Responders Public Safety Homeland Security Bureau*. <http://www.fcc.gov/pshs/docs/public-safety-spectrum/031710/Newman-Peha-PSHS-21century-comm-031710.pdf>
- [NPST1] National Public Safety Telecommunications Council (NPSTC) *Public Safety 700MHz Broadband Statement of Requirements*, Nov 8, 2007. <http://www.npstc.org/documents/Public%20Safety%20700MHz%20Broadband%20SoR%20v0.6.pdf>
- [NPST2] NPSTC, 700 MHz Public Safety Broadband Task Force Report and Recommendations, Sep. 2009. http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf
- [NSEP] National Security/Emergency Preparedness (NS/EP), *Internet Protocol (IP) Multimedia Subsystem (IMS) Core Network Industry Requirements (IR) for Next Generation Network (NGN) Government Emergency Telecommunications Service (GETS)*, Phase 1, Voice Service, Dec 2009. <http://www.ncs.gov/library/misc/NSEP%20IMS%20Core%20Network%20IR%20-%20Issue%201%200%20public.pdf>
- [NYC] New York City, Fire Department, Police Department, Information Technology and telecommunications, *700 MHz Broadband Public Safety Applications and Spectrum Requirements*, Feb. 2010. <http://andrewseybold.com/wp-content/uploads/2010/03/700MHz-Whitepaper-on-Spectrum-Feb-2010-FINAL.pdf>
- [OB12] OBI Technical Paper No. 2, FCC, *A Broadband National Cost Model*. <http://www.fcc.gov/pshs/docs/ps-bb-cost-model.pdf>
- [OIT] Office of Information Technology, NJ, *Request for Information (RFI) for 700 MHz Public Safety Network*, 2010. http://www.state.nj.us/treasury/pdf/700MHz_Public_Safety_Network_RFI.pdf
- [OIC] Office for Interoperability and Compatibility, *Public Safety Statements of requirements*, Aug 2008. <http://www.emsa.ca.gov/systems/files/sorv1.pdf>
- [PEHA] Peha, J and Sutivong, A, *Admission Control Algorithms for Cellular Systems*, ACM/Baltzer Wireless Networks, 1999
- [PSCR1] Public Safety Communications Research, *Inaugural Stake Holders Meeting*, Mar 15, 2010, Boulder, CO. http://www.pscr.gov/projects/broadband/700mhz_demo_net/inaug_stakeholder_mtg_042010/inaug_stakeholder_mtg_042010.php

- [PSCR2] Public Safety Communications Research, *Winter 2010 Public Safety 700-MHz Demonstration Network Stakeholder Meeting*, Dec 1 – 2, 2010, Boulder, CO. http://www.pscr.gov/projects/broadband/700mhz_demo_net/stakeholder_mtg_122010/stakeholder_mtg_122010.php
- [PSCR3] Public Safety Communications Research, *Priority, Preemption, and QoS*, in [PSCR1]. http://www.pscr.gov/projects/broadband/700mhz_demo_net/stakeholder_mtg_122010/day_1/5.1_qos_priority_preemption-pscr_intro.pdf
- [PSST1] Public Safety Spectrum Trust, *Private/Public Partnership, Bidder Information*, Nov 30, 2007. http://www.psst.org/documents/BID2_0.pdf
- [PSST2] Public Safety Spectrum Trust, *Minimum Requirements for Local/Regional Public Safety Buildout*, Dec 15, 2009. <http://www.psst.org/documents/PSST-Minimum-Recommendations-121509.pdf>
- [ROBE] Roberson and Associates, *Whitepaper: Technical Analysis of the Proposed 700 MHz D-Block Action*, Aug 23, 2010. <http://fjallfoss.fcc.gov/ecfs/comment/view?id=6015952735>
- [SAFE] The Safecom Program, *Public Safety Architecture Framework*, Feb 10, 2006. http://www.pscr.gov/outreach/safecom/psaf/psaf_docs.php
- [SESI] Sesia, S, Taufik, I, and Baker, M, *LTE – A Pocket Dictionary of Acronyms*, Wiley. 2009. http://lte.alcatel-lucent.com/locale/en_us/downloads/LTE-A_Pocket_Dictionary_of_Acronyms.pdf

Acronyms²

3GPP: 3rd Generation Partnership Project

AAA: Authentication, Authorization,
Accounting

AC: Access Class

ACB: Access Class Barring

AF: Application Function

ARP: Allocation and Retention Priority

AVL: Automatic Vehicle Location

CAN: - Connectivity Access Networks

CODEC: COder – DECoder

DPI: Deep Packet Inspection

EC: Establishment Cause

EIR: Equipment Identity Register

EPC: Evolved Packet Core

EPS: Evolved Packet System

FCC: Federal Communications Commission

GBR: Guaranteed Bit Rate

GERAN: GSM/EDGE Radio Access Network

GETS: Government Emergency
Telecommunications Service

GPS: Global Positioning System

Gx: Interface between PCRF and P-GW

HB: Hand Back

HLR: Home Location Register

HO : Hand Over

HSS: Home Subscriber Server

ICS : Incident Command System

IETF: Internet Engineering Task Force

IMS: IP Multimedia Subsystem

IMSI : International Mobile Subscriber
Identity

IOT : Inter Operator Testing

IP: Internet Protocol

LI: Legal Intercept

LMR: Land Mobile Radio

LTE: Long Term Evolution

MBR: Maximum Bit Rate

ME: Mobile Entity

MME: Mobility Management Entity

MMS: Machine to Machine System

MOCN: Multi Operator Core Network

MPS: Multimedia Priority Service

NBDS: Nationwide Broadband Data System

NBP: National Broadband Plan

NCL: Neighbor Cell List

NIST: National Institute of Science and
Technology

² A very concise and useful annotated 3GPP standards vocabulary is available in [3GPP1]; Also see [SESI] for an annotated list of comprehensive LTE Acronyms

NTIA: National Telecommunications and Information Administration

NPSTC: National Public Safety Telecommunications Council

NSA: Network Service Agreement

OA&M: Operations, Administration, and Management

PCC: Policy and Charging Control

PCEF: Policy and Charging Enforcing Function

PCRF: Policy and Charging Rules Function

PDN: Public Data Network

P-GW: PDN GateWay

PLMN: Public Landline Mobile Network

PS: Public Safety

PSCR: Public Safety Communications Research

PSST: Public Safety Spectrum Trust

PSTN: Public Switched Telephone Network

PSBL: Public Safety Broadband Licensee

PSPDN: Public Safety Private Data Network

QCI: QoS Class Indicator

QoS: Quality of Service

RAC: Radio Admission Control

RACH: Random Access CHannel

RAN: Radio Access Network

RAT: Radio Access Technology

RB: Radio Bearer

RNS: Radio Network Subsystem

RRC: Radio Resource Control

Rx: Reference Point between AF and PCRF

S1-MME: Control Plane Interface between eNodeB and MME

S1-U: User Plane Interface between eNodeB and S-GW

S3: Bearer Interface between MME and SGSN

S4: Interface for Mobility Support between SGSN and S-GW

S5: Interface for user plane between S-GW and P-GW

S6a: Subscriber related Interface between MME and HSS

S8: Interface between Visitor PLMN S-GW and Home PLMN P-GW (variant of S5)

S9: Interface between Home PCRF and Visitor PCRF

S10: Reference point between MMEs

S11: Control traffic interface between MME and S-GW

S12: User plane interface between UTRAN and S-GW

SGi: Reference Point between P-GW and PDN

SDF: Service Data Flow

SGSN: Serving GPRS Support Node

S-GW: Serving GateWay

SIB: System Information Block

SIP: Session Initiation Protocol

SLF: Subscription Location Function

SM: Session Management

SMS: Short Message System

SPR: Subscriber Profile Repository

SU: Software Upgrade

TA: Tracking Area

TCP: Transmission Control Protocol

TFT: Traffic Flow Template

UDP: Universal Datagram Protocol

UE: User Equipment

UICC: Universal Integrated Circuit Card

UMTS: Universal Mobile Terrestrial System

USIM: Universal Subscriber Identity Module

UTRAN: UMTS Terrestrial Radio Access Network

Uu: Air Interface between UE and e-UTRAN

VPN: Virtual Private Network

VoIP: Voice over Internet Protocol

X2-C: Control Plane Interface between two
eNodeBs

X2-U: User Plane Interface between two
eNodeBs

Appendix A: LTE/EPC Overview and Priority Mechanisms

A.1 LTE/EPC Introduction

LTE and EPC are part of the 3rd Generation Partnership Project (3GPP) Standards (www.3gpp.org). It is the next step in technology from the 3G standards, i.e., Wideband Code Division Multiplexing / High Speed Packet Access (WCDMA/HSPA). Estimates indicate that LTE will likely provide 25 Mbps (DL) and 10 Mbps (UL) in a 5 MHz band. The overall architecture has been introduced in Figure 3.1.

The eNodeB provides radio access and management functions and the Radio Bearer (RB) to the User Equipment (UE). Its functions include Radio Admission Control (RAC), Radio Resource Management (RRM), encryption and compression, air interface mobility / Hand Over (HO), Radio Bearer (RB) control, connection mobility control, dynamic allocation of resources to UEs in uplink and downlink, scheduling, and security.

The backhaul between the RAN and EPC core is the Internet Protocol (IP) based S1 Interface [3GPP16, Sec. 19].

The Evolved Packet Core (EPC) manages and delivers a personalized subscriber experience, supports and introduces new equipments and applications, and provides support for seamless mobility and service portability across wireless IP networks. In the following, its major constituents are described.

MME performs the bearer management control functions to establish the (radio) bearer paths that the UE uses. The MME contains the signaling and control functions to manage the UE access to network connections, the assignment of network resources, and the management of mobility states to support tracking, paging, roaming, and HOs. It has the capability to reject requests from UEs under overload [3GPP10, Sec. 4.3.7.4]. The MME dynamically stores the UE context information [3GPP10, Sec. 5.7.2].

S-GW maintains the Evolved Packet System (EPS) bearer context information for User Equipment (UE) [3GPP10, Sec. 5.7.3].

P-GW includes the Policy and Charging Enforcing Function (PCEF) for enforcing the priority rules provided by PCRF. It also maintains the EPS bearer context information for UEs [3GPP10, Sec. 5.7.4].

PCRF derives QoS requirements from service description, makes QoS decisions, and supports Service Data Flow (SDF) detection, policy enforcement, and flow-based charging. The PCRF provides real-time network, application, and subscriber policies. It makes available flexible per-session, per-subscriber, and per-application policy controls. It provides adaptive policy controls to manage network bandwidth usage in-session. The PCRF parameter mapping functions are defined in [3GPP13, Sec. 6.3].

The HSS is a concatenation of the traditional Home Location Register (HLR) and the Authentication Center (AuC) from the WCDMA/HSPA world. The HSS is in charge of generating security information used for terminal authentication and radio link ciphering and integrity protection [3GPP14, Sec. 5]. It also contains user information related to service provisioning and additional value added capabilities.

Associated with the HSS are the Equipment Identity Register (EIR), integrated Subscription Location Function (SLF), and support for Lawful Intercept (LI). The EIR is responsible for Mobile Entity (ME) identity check procedure [3GPP14, Sec. 6].

The Operations, Administration, and Management (OA&M) console provides network management and control, and also user provisioning and management functions.

The key interfaces in the LTE/EPC complex [3GPP10, Sec. 4.2.3] are summarized below.

S1-MME: Reference point for the control plane protocol between E-UTRAN and MME.

S1-U: Reference point between E-UTRAN and S-GW for user traffic.

S3: Reference point between MME and SGSN to enable user and bearer information exchange for inter 3GPP network mobility.

S4: Reference point between S-GW and SGSN to provide control and mobility support and user plane tunnelling.

S5: Reference point between S-GW and P-GW to provide user plane tunnelling and tunnel management.

S6a: Reference point between MME and HSS for authenticating/authorizing user access.

Gx: Reference point between PCRF and PCEF in P-GW for transfer of QoS policy and charging rules.

S8: Reference point providing user and control plane between the S-GW in the visitor PLMN and the P-GW in the home PLMN. S8 is the inter PLMN variant of S5.

S9: Reference Point for transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function.

S10: Reference point between MMEs for MME relocation and MME to MME information transfer.

S11: Reference point between MME and Serving GW.

S12: Reference point between UTRAN and S-GW for user plane tunnelling

SGi: Reference point between the P-GW and the PDN.

Rx: Reference point between the AF and the PCRF.

Uu: Air Interface between UE and E-UTRAN.

A.2 User Equipment (UE)

The major attributes for identifying UEs are bandwidth, operational frequency bands, and power.

LTE defines three classes for UEs [3GPP16, Annex G] depending upon the bandwidth capabilities expected as shown in Table A.1. The public safety community may need to decide on the UE class for their needs.

Table A.1: UE Classes

Class	UL	DL
A	[50] Mbps	[100] Mbps
B	[25] Mbps	[50] Mbps
C	[2] Mbps	[2] Mbps

[3GPP7, Sec. 5] identifies the operating bands for LTE Evolved-Universal Terrestrial Radio Access (E-UTRA). The E-UTRA operating bands relevant to the 700 MHz spectrum region in the U.S. are shown in Figure A.1.

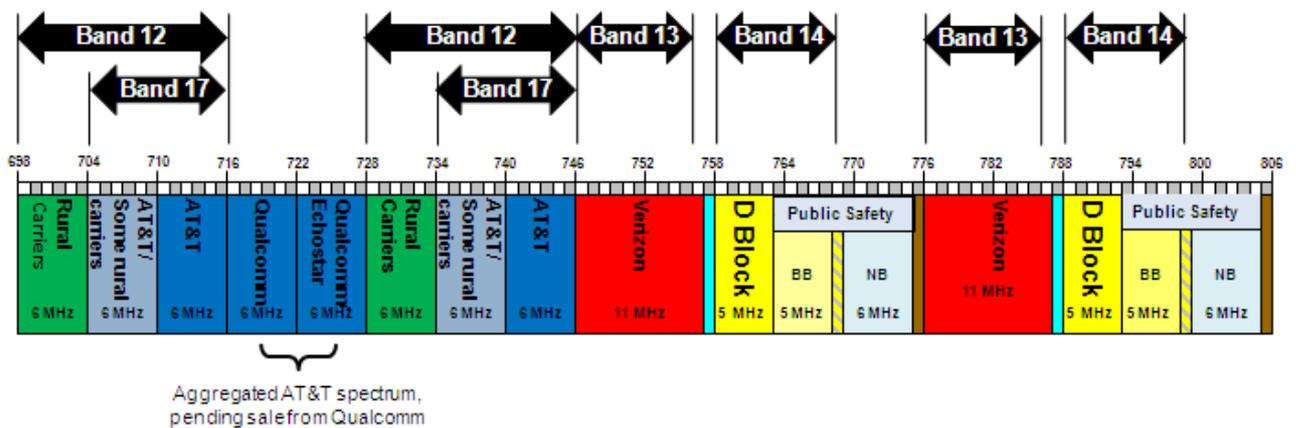


Figure A.1: 700 MHz E-UTRA Operating Bands

In addition to identifying the intended frequency bands for the LTE standard, the E-UTRA operating bands are used by manufacturers of base transceiver (eNodeB), user equipment (UE), and their component parts, to specify in which frequency regions their devices are designed to operate. For example, UE components such as transmitters and transmit filters might be designed to operate in only one E-UTRA operating band class, or could be designed to operate in multiple E-UTRA operating bands.

In order for public safety UE to operate on commercial networks as well as on the dedicated public safety broadband network, it is necessary that public safety devices be able to operate in all the 700 MHz LTE E-UTRA operating bands indicated in Figure A.1. In order to achieve the desired low cost for public safety user devices, it is desirable that all 700 MHz LTE devices be capable of all 700 MHz band classes. This will allow public safety devices to share the large commercial volumes for the entire 700 MHz region, and enjoy the same economies of scale as commercial devices. This recommendation has also been stated in the FCC Whitepaper [FCC2].

From power capability viewpoint, the supported UE is defined to be power class 3 (23 dBm, 1/5 W) [3GPP7, Table 6.2.2-1].

For inter-frequency HO, data reception and neighbor cell search need to be carried out at different frequencies. The 3GPP standards facilitate this by providing gaps in the data transmission, during which the terminal can retune to a different frequency for inter-frequency measurement purposes. This avoids the necessity of equipping a UE with separate RF receiver circuitry,

The UE has a radio capability which is sent to the MME via the eNodeB when requested during the initial context request procedure. It includes the frequency band capabilities of the UE. Also the UE has core network related capability, in particular security algorithms. The context information associated with the UE is summarized in [3GPP10, 5.7.5].

A.3 Connections, Session Establishments, and Hand Overs

The operations in the RAN and core entities can be classified into two types of protocol-based activities: Control Plane (C-Plane) and User Plane (U-Plane). The C-Plane consists of protocols for control and support of the user plane functions. The U-Plane is responsible for delivery of user data (traffic bearer).

The UE, after powering up, needs to acquire time and frequency synchronization with a cell and detect the physical layer cell ID of that cell through the cell search procedure or synchronization procedure. The UE initiates the system acquisition and signaling setup which includes the Radio Access CHannel (RACH) procedure [3GPP16, Sec. 10.1.5] and Radio Resource Control (RRC) procedure.

The purpose of the RACH procedure is to establish link synchronization and also a unique terminal identity. It includes the transmission of a contention-resolution message from the eNodeB to the terminal. This helps to resolve any contention due to multiple terminals trying to access the eNodeB

using the same random access resource. A UE can access the target cell via RACH following a contention free procedure using a dedicated RACH preamble [3GPP16, Secs. 10.1.2.1, 10.1.5.1].

RRC which resides in eNodeB takes care of RRC connection management, radio bearer control, mobility functions, and UE measurement reporting and control. This is followed by registration and security. These include authentication [3GPP11, sec. 5.4.2], and security and location management [3GPP10, Sec. 5.3]. Attach [3GPP10, Sec. 5.3.2] and IP Address Assignment [3GPP11, Sec. 6.2] are carried out during establishment of the default bearer. Same IP address is used for dedicated bearer. The Attach procedure [3GPP11, Sec. 5.5.1] results in creation of the default bearer activation [3GPP11, 6.4.2, Sec. 6.5]. This may be followed by service request and QoS handling which creates a dedicated bearer activation followed by traffic exchange and bandwidth management. Associated message contents and their structures are provided in [3GPP16, Sec. 8].

Subsequent to the completion of a session, the UE may detach and enter into the Idle mode.

When a UE needs to move to another RAN, mobility and HO operations are invoked.

HOs involve moving into a target eNodeB or network as a result of weak signal, or for overload situations from an existing connection in a source network. The types of the HO depend on the nature of the application, whether the applications requires stringent packet error rate control, e.g., data or comparatively non-stringent error rate, e.g., streaming video, and whether the HO is intra- or inter-network.

The relocation/HO procedures need to include processes that precede the final HO step on the source network side e.g., evaluation of UE and eNodeB measurements, preparation of resources on the target network side, commanding the UE to the new radio resources, and finally releasing resources on the (old) source network side. The procedures contain mechanisms to transfer context data between eNodeBs and to update node relations on C-plane and U-plane.

HO signaling procedures are available in LTE for both inter-eNodeB and inter-Radio Access Technology (RAT) situations. The specifications cover both S1 and X2 based HO. A mathematical analysis of various algorithms is covered in [PEHA].

S1 based HO [3GPP10, Sec. 5.5.1.2] generally applies when the X2 connectivity is not present between the source and the target eNodeBs [3GPP16, Secs. 10.1.2.1.1, 19.2.2.5]. The MME is actively involved in the HO process (see Figure A.2). Also, refer to [3GPP16, Fig. 10.1.2.1.1-1] which deals with X2 based HO but can be extended to S1 based HO wherein the communications between the two eNodeBs is through the MME instead of being directly across the X2 interface

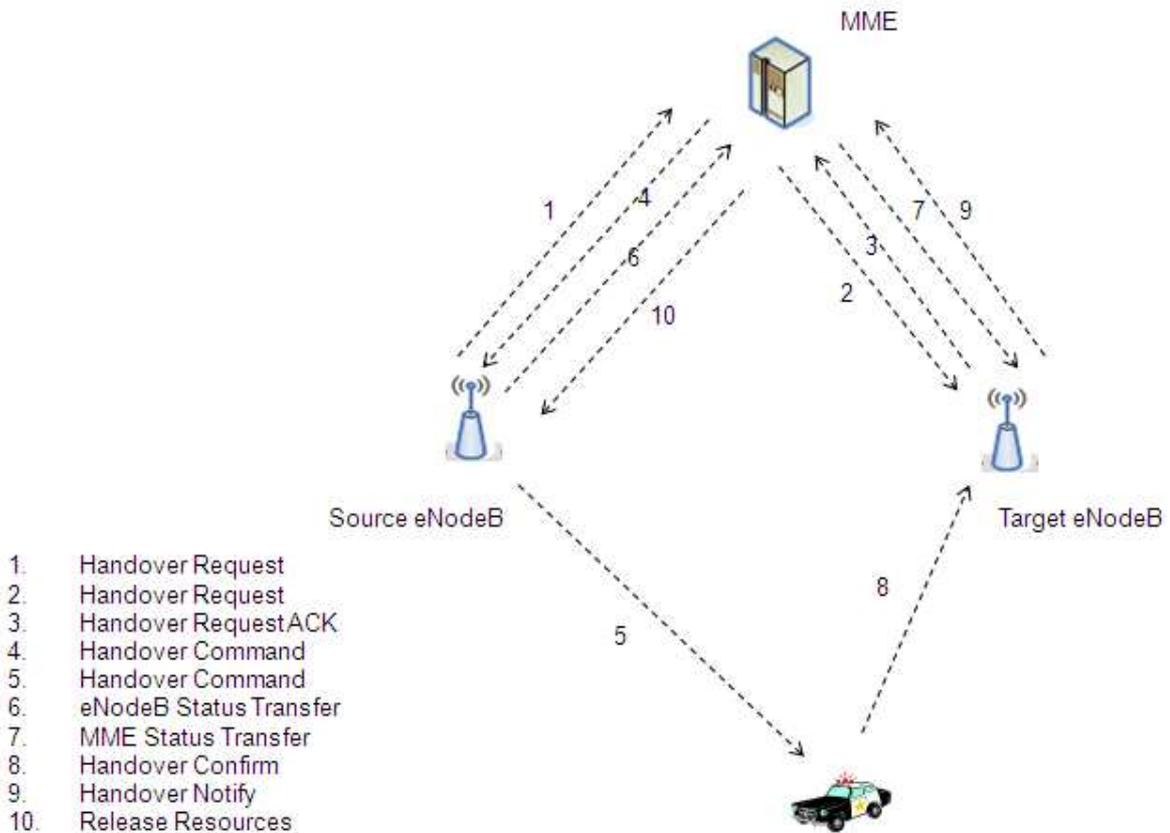


Figure A.2: S1 Based Hand Over (HO)

The key steps are summarized in the following

1. The HO required message is sent by the source eNodeB to the MME.
2. The MME sends the HO request message including the E-RAB(s) which need to be set up by the target eNodeB.
3. The target eNodeB responds with the HO Request ACK message after the required resources for all accepted E-RABs are allocated.
4. The MME sends the HO command message to the source eNodeB.
5. The eNodeB follows up with sending the HO command to the UE. The HO preparation phase is complete.
6. The source eNodeB sends the status information to the MME for transmittal to the target eNodeB.
7. The MME passes on the received status information to the target eNodeB.
8. The UE sends the HO confirm message to the target eNodeB.
9. The HO notify message is sent by the target eNodeB to the MME when the UE has successfully been transferred to the target eNodeB.
10. The MME then suggests to the source eNodeB to release the resources associated with the UE.

The associated path switch steps and details of user traffic flow are available in [3GPP16, Sec. 19.2.2.5], [BAJZ].

Clearly, a more efficient and faster HO is based on use of the X2 connectivity [3GPP10, Sec. 5.5.1.1] if present, between the source and the target eNodeBs, [3GPP16, 20.2.2.1]. Here, the MME is minimally involved in the activities except for directing the S-GW to change the user traffic path towards the target eNodeB upon when the HO procedure has been executed and the scenario is in the completion phase (see Figure A.3). See also [3GPP16, Fig. 10.1.2.1.1-1], [3GPP10, Fig. 5.1.1.1.2-1].

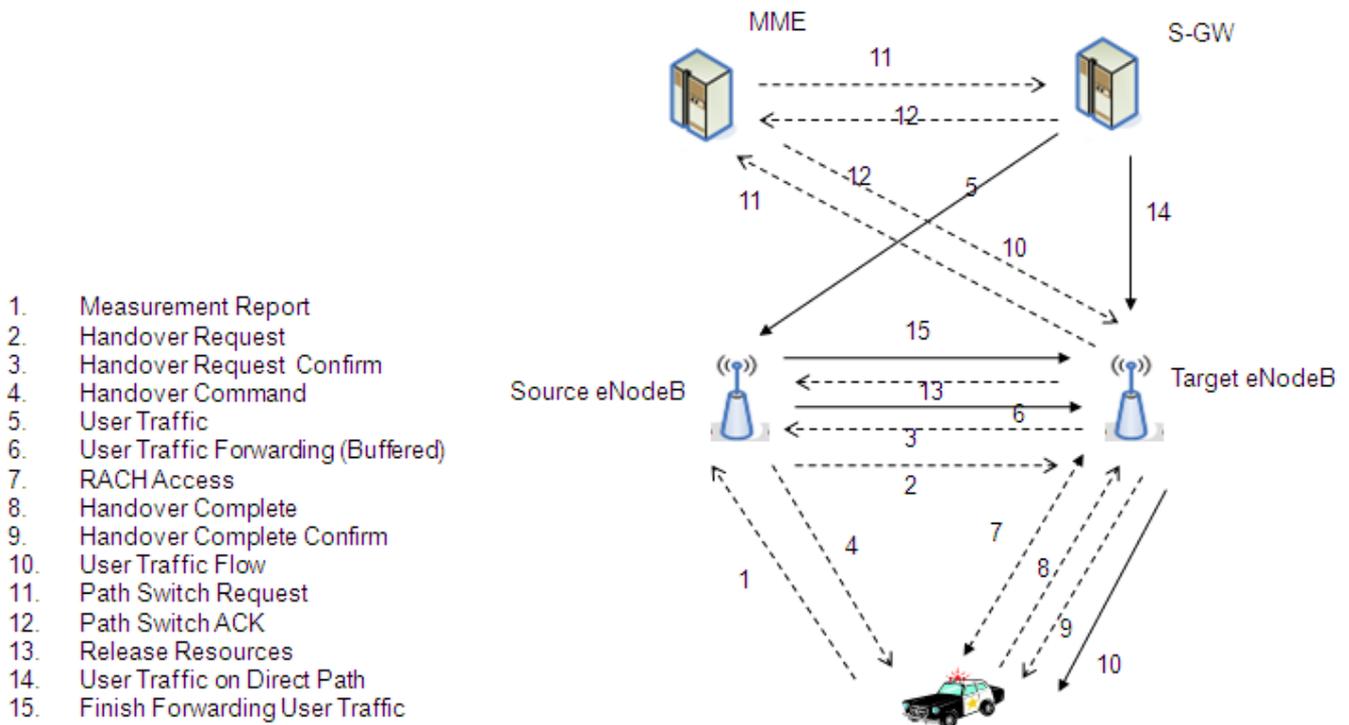


Figure A.3: X2 Based Hand Over (HO)

1. While the UE is being served by the source eNodeB, it is providing the measurements reports for possible a HO. It may be noted that inter frequency measurements are also possible [3GPP16, Sec. 10.1.3].
2. The HO preparation is initiated by the source eNodeB by sending a HO Request to the target eNodeB including the bearer setup by the target eNodeB.
3. The target eNodeB works with the MME and S-GW to set up resources for the UE. The target eNodeB responds with the HO Request Ack/Confirm, resulting in the completion of the HO preparation phase.
4. The source eNodeB sends a HO command to the UE. While the UE completes the various RAN related HO procedures, the source eNodeB starts the status and data transfer to the target eNodeB.

5. Prior to the HO, the user traffic is being sent by the S-GW to the source eNodeB.
6. The source eNodeB directs the user traffic across the X2-U interface to the target eNodeB in order to ensure that subsequently, the UE will receive all the packets. This may create gap (e.g., jitter) for packet arrival stream to the UE but the packet loss will be minimized.
7. The UE completes the RACH procedure with the target eNodeB.
8. The UE sends the HO complete message to the target eNodeB.
9. The target eNodeB sends the HO complete confirm message to the UE.
10. The user traffic flow switches to the target eNodeB based on the buffered packets received from the source eNodeB.
11. The MME sends the path switch request to the S-GW after receiving the request from the target eNodeB.
12. The S-GW sends the path switch acknowledge to the MME.
13. When the data path in the user plane is switched, the target eNodeB sends a message to the source eNodeB to release the resources originally used by the UE.
14. The direct user traffic path has been established between the S-GW and the target eNodeB.
15. The source eNodeB finishes sending the user traffic to the target eNodeB.

It may be noted that, in case of congestion in the target eNodeB, the user can receive the priority treatment in the source eNodeB. Several mechanisms are available to handle such situations and to avoid unnecessary steps. These include the following:

- Both the source eNodeB and the UE to keep some context information to enable return of the UE in case of HO failure [3GPP16, Sec. 10.1.2.1].
- eNodeBs can request load information from another eNodeB (across the X2 interface) and not even attempt to hand over to the target eNodeB [3GPP16, Sec. 20.2.2].
- Target eNodeB can send a HO preparation failure message to source eNodeB upon receiving HO preparation request message [3GPP16, Sec. 20.2.2.1].

Roaming [3GPP10, Sec. 4.2.2] is defined as the situation wherein a user is operating on a network other than its normal home network, on a temporary or “nomadic” basis. After a user equipment connects to a visitor network, the visitor network performs authentication and authorization in cooperation with the HSS in the UE’s home network. The user traffic in the visitor network can be handled in two ways: the Home Directed traffic and the Local Breakout traffic approach. In case of Home Directed traffic, the bearer is set up between the visited S-GW and the home P-GW (S8 interface) and hence the user traffic is directed through the home network core. For the Local Breakout approach, the user traffic uses the core bearer facilities (S5) in the visited network.

A.4 LTE/EPC Priority Mechanisms

A.4.1 Access to Air Interface and Attach Activities

Admission is based on the Access Class (AC) value for the UE [3GPP2, Secs. 4.2, 4.3], [LIND]. The recommended allocations of access priorities are summarized in Table A.2 [3GPP4, Table 6.1].

Table A.2: Radio Access Priority (Suggested in 3GPP)

Access Class	Usage	Applicability
15 (highest)	Reserve, PLMN Staff	HPLMN only
12 – 14	Public Safety	Home and Visited PLMN's (Home country)
11	Reserve, PLMN Staff	HPLMN only
10	Emergency (non PS users)	Home and Visited PLMNs
0 -9	General Use	Home and Visited PLMNs

Access priority classes 15 and 11 are reserved for the PLMN operator for emergency and other maintenance and administrative uses. The set of lowest priorities 0 – 9 are randomly assigned to commercial users and all commercial users are treated in equal fashion. Level 10 is reserved for emergency situation (e.g., equivalent of a 911 call) for the commercial users. That leaves three priority levels 12 – 14 for use by the public safety community.

System information is provided by eNodeB in the form of information blocks [3GPP17, Sec. 6]. System Information Block 1 (SIB1) contains relevant information when evaluating if a UE is allowed to access a cell and defines the scheduling of other system blocks. eNodeBs implement RAC using the associated Access Class Barring (ACB) parameters: BarringForSpecial for priority users; BarringForEmergency for users with emergency; and the low BarringFactor for commercial users [3GPP17, Sec 6.3.1]. The eNodeB broadcasts the System Information Block 2 (SIB2) with ACB information, and the UE uses its AC in the USIM to evaluate access permissions [3GPP17, Sec. 5.2.2].

BarringFactor parameter is used by the commercial users in the access class 0 – 9. If the random number drawn by the UE is lower than this value, access is allowed. Otherwise access is barred. The values are interpreted in the range [0,1]: p00 = 0, p05 = 0.05, p10 = 0.10, ..., p95 = 0.95. All commercial users can be barred by eNodeB by setting p = 00. Re-attempts are delayed based on the ac-BarringTime delay parameter provided by the eNodeB [3GPP2, Sec. 4.3], [3GPP17, sec. 6.3.1]. BarringForEmergency (Boolean value) is used for Emergency calls (access class 10).

BarringForSpecial applies to ACB for AC 11-15. The first/ leftmost bit is for AC 11, the second bit is for AC 12, and so on. These can be selectively set to zero or one by the eNodeB.

In order to be an effective mechanism to meet the needs of public safety user, ACB can be dynamically controlled based on the congestion experienced within the network and become active without manual service provider intervention.

It may be necessary to reiterate that the network nodes will not give priority based on just the AC values. The priority treatment depends on what is being exempted from the AC barring test. If two AC values are exempted from the AC barring test, then those AC values are treated in the same way. This is true even if those two AC values are 15 and 1.

For Radio Resource Control (RRC) connection initiation, Establishment Cause (EC) is used. This can be set as HighPriorityAccess for public safety and operator classes (11 – 15), Emergency for emergency class (10), and Mobile Originating for commercial user classes (0 – 9) [3GPP17, Sec. 5.3.3.2]. RRC requests are prioritized via use of the Establishment Cause set to “HighPriorityAccess” for each “RRCConnectionRequest” from a public safety user. For commercial UE, upon receipt of the “RRCConnectionRequest”, the eNodeB may respond with an “RRCConnectionReject” if it cannot allocate resources. Following receipt of an “RRCConnectionReject” message, the commercial UE may not attempt another “RRCConnectionRequest” for a period of time based on the “wait time” specified by the eNodeB in the RRC reject message.

In addition, the eNodeB may check its ability to accept a Radio Bearer (RB) setup request (including HO and RRC connection re-establishment) based on certain factors including Maximum Number of UE’s and Radio Bearers (RB’s), Number of Radio Bearers (RB’s) on Guaranteed Bit Rate (GBR), and hard capacity limit.

Many options exist to determine the QCI and ARP parameters assignment to the default bearer during Attach. The parameters may be downloaded from the HSS, based on static policy rules within the P-GW, or based on dynamic policy rules installed in a PCRF. Normally, the QoS characteristics of the default bearer are determined by the subscription as stored in the HSS.

The establishment of a dedicated bearer triggered by a service or application request is the next key step.

A.4.2 Dedicated Traffic Bearer on Request

Guaranteed Bit Rate (GBR) bearers are bearers for which dedicated network resources are permanently allocated [3GPP16, Sec. 13] to guarantee the committed bandwidth.

Maximum Bit Rate (MBR) reflects the maximum network resources to be allocated to the user. In LTE release 8, GBR and MBR are made equal to each other.

Aggregated Maximum Bit Rate (AMBR) sets the limitations on the maximum bandwidth for all the bearers assigned to the UE. AMBR is the maximum data rate that cannot be exceeded for a UE.

The Allocation and Retention Priority (ARP) [3GPP8, Sec. 6.1.7.3] contains information about the priority level (scalar), the preemption capability (flag) and the preemption vulnerability (flag).

ARP Priority level is the entry level gate for establishing a bearer. It is typically stored in subscriber’s HSS profile. The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority. ARP controls how the eNodeB reacts when there are insufficient resources to establish a

new Radio Bearer (RB). In case of limited resources, the eNodeB attempts to preempt an existing RB and accept the new RB request depending upon the other two flags. This process is especially useful in disaster situations wherein existing lower priority commercial users in a network can be preempted. Once successfully established, a bearer's ARP value has no effect on the packet forwarding treatment (e.g. scheduling and queue management) a bearer receives. These are affected by the QoS Class Indicator (QCI) as discussed later in this section.

The ARP pre-emption capability flag defines whether the bearer could preempt another lower ARP priority level bearer to free up the required resources. The flag may be designated as "Yes" for high priority users, e.g., public safety users, and "No" for lower priority users, e.g., commercial users. The ARP preemption vulnerability flag defines whether this bearer is a candidate for preemption by a preemption capable bearer with a higher ARP priority value. It may be set as "No" for high priority users and "Yes" for lower priority users.

The service or application oriented parameter, independent of the ARP priority of a user, is the QoS Class Identifier (QCI). QoS mechanisms are well defined in [3GPP16, Sec. 13]. QCI dictates the packet-level preferential treatment a bearer receives. It ensures that high priority applications will be allocated resources at the expense of lower priority applications. Different user members of a specific bearer class receive the same bearer level packet forwarding treatment (e.g., round robin scheduling, queue management policy, and rate shaping policy) [3GPP16, Sec. 13] independent of their ARP values.

A typical application type may be associated with a specific Guaranteed Bit Rate (GBR) or N-GBR QCI value and the associated EPS bearer is treated with a corresponding packet management treatment (see Table A.3) [3GPP9, Table 6.1.7].

Table A.3: QCI to Packet Priority Mapping

Service Example	QCI	Priority
Conversational Voice	1 (GBR)	2
Conversational Video	2 (GBR)	4
Robotics	3 (GBR)	3
Streaming Video	4 (GBR)	5
IMS Signaling	5 (N-GBR)	1
WWW, Email, ftp, ...	6 (N-GBR)	6
Voice, Interactive Gaming	7 (N-GBR)	7
WWW, Email, ftp, ...	8 (N-GBR)	8
WWW, Email, ftp, ...	9 (N-GBR)	9

For packet level treatment for different applications with their related QCI values, the range of priorities is 1 to 9 with 1 as the highest. As is clear from Table 3.3, the order of the QCI value does not necessarily map into the corresponding priority order although there is a one-to-one mapping between the two.

There are two types of bearers defined in LTE/EPC standards: default bearer and dedicated bearer.

A default bearer is established when the UE connects to a PDN, and remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity. A default bearer is always a Non-Guaranteed Bit Rate (Non-GBR) bearer [3GPP16, Sec. 13]. The QoS parameter values for the default bearer for a user are based on the user's subscription data and are stored in the home HSS.

Dedicated bearer is any additional EPS bearer/E-RAB that is established in order to support a service / application request. It can either be a GBR or a Non-GBR bearer. Illustrative flowchart on bearer establishment is provided in [3GPP10, Sec. 5.4.1].

The UE initiated bearer change request is available in [3GPP13, Sec. 6.1.1].

These parameters and attributes determine the activities and process for implementing the priority treatment as indicated in the following.

A.4.3 Priority Treatment Activities

Priority treatment primarily focuses on the management of resources, the primary measure of which is the bandwidth associated with the bearer request. Other “capacity” attributes may be applicable for individual elements, e.g., number of UEs, database entries.

The key elements associated with PCC rules [3GPP12, Sec. 4.3] are the Policy and Charging Rules Function (PCRF), Policy and Charging Enforcement Function (PCEF), Subscriber Profile Repository (SPR), and Application Function (AF) [3GPP12, Fig. 4.1] (see Figure A.4).

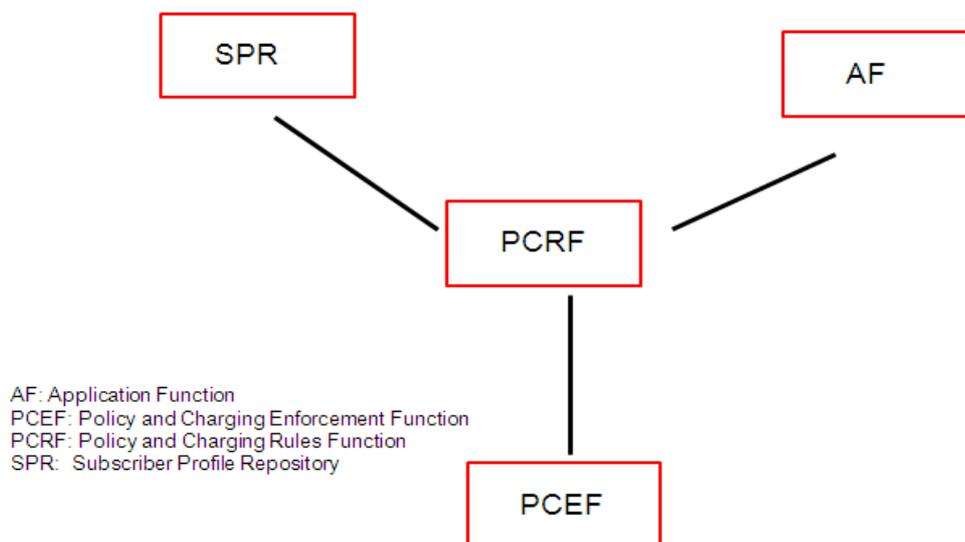


Figure A.4: Policy and Charging Control (PCC) Elements

As indicated in Sec. 3.1, the PCRF authorizes QoS resources. It uses the service information received from the AF and/or the subscription information received from the SPR to calculate the proper QoS authorization (QCI, bitrates). The PCRF may also take into account the requested QoS received from the PCEF. During default bearer creation, the ARP for the default bearer provided by the HSS may be modified by the PCRF/SPR using a PCC rule which considers the service user’s priority level. Representative pseudo-code and algorithms are available in [3GPP13, Sec. 6.3].

The PCEF, located as part of the P-GW, interfaces with the PCRF through the Gx interface [3GPP12]. It is used for the transmission of traffic plane events to the PCRF and for enforcement of the rules in the EPC.

The SPR [3GPP8, Sec. 6.2.4] contains subscriber information needed by the PCRF for developing subscription-based policies and IP-CAN bearer level PCC rules for IP-CAN establishment [3GPP13, 4.1]. It may be combined with other databases in the system, e.g., HSS. It provides subscriber

category, subscriber's allowed service with associated preemption priority, subscriber guaranteed bandwidth QoS, and subscriber's charging related information.

The AF forwards service description to PCRF. It reports session events (e.g. session termination, modification [3GPP8, Sec. 4.3.2]) and is involved with PCRF for the right treatment for multimedia and dynamic application changes. An illustration of how AF is involved in the service request procedure is available in [3GPP11, Sec. 5.6.1].

In general, the PCC rules for data rate, QCI, and ARP assignment may be based on the following precedence (3GPP13, Table 6.3.1):

1. As defined by operator specific algorithm.
2. As defined by application specific algorithm.
3. As defined by COder – DECoder (CODEC) specific algorithm.

For a given environment with range of users, the network operator needs to ascribe these parameters and attributes. The mappings are at the discretion of the operator and in many instances, these can be n-to-m, i.e., there is not necessarily a one to one mapping as different attributes are assigned. A representative template for assignments for the priority attributes is shown in Table A.4.

Table A.4: Priority Attributes Assignment Template

Radio Admission and Bearer Creation (User dependent)					
User "Types"	Subscriber Priority	Radio Admit	Bearer Alloc. & Retain		
		RAC Priority (15 highest)	ARP Pr. (1 Highest)	Pre-empt Others	Pre-empt Vulnerable
UT1	SP1	15	1	YES/NO	YES/NO
...
Utn	SPn	1	15	YES/NO	YES/NO

Bearer QoS Treatment (Dependent only on application)			
Application Example	Service Class	QCL (1 – 9)	Treatment Priority (1 highest)
App	Convers voice	1 (GBR)	2
System	IMS Signaling	5 (N-GBR)	1
...
Appn	WWW, email, ...	9 (N-GBR)	9

Given a set of user types UT1 to UTn, one can assign a range of subscriber priorities SP1 to SPm.

The first set of LTE assignments pertain to the Radio Admission Control (RAC). 15 is the highest and 0 is the lowest value. In order to establish the corresponding QCI related bearer, one needs to assign the ARP attributes. The ARP attributes range from 1 to 15 with 1 being the highest. The associated “preempt others” (y/n) and “preempt vulnerability” (y/n) flags can then be assigned for subscribers SP1 to SPm.

The next set of assignments can be the QCI values depending upon what service or application the user wants to invoke. Depending upon the service or application, a service class QCI value from Table A.3 may be assigned. An illustrative example of application of these mappings is shown in the Figures A.5 and A.6. It is assumed that the public safety and the commercial users are invoking the same application.

Initially, a non-congested network is assumed where the resources are still available for any type of users. In such an environment, the bearer can be established for both the public safety and the commercial users. Based on the availability of the resources in the corresponding bearer associated with the QCI value of 3, the ARP priority need not be invoked and both users end up being assigned the GBR bearer (See Figure A.5). Within the Application 3 bearer, both users may get the same packet scheduling treatment, e.g., round robin packet scheduling.

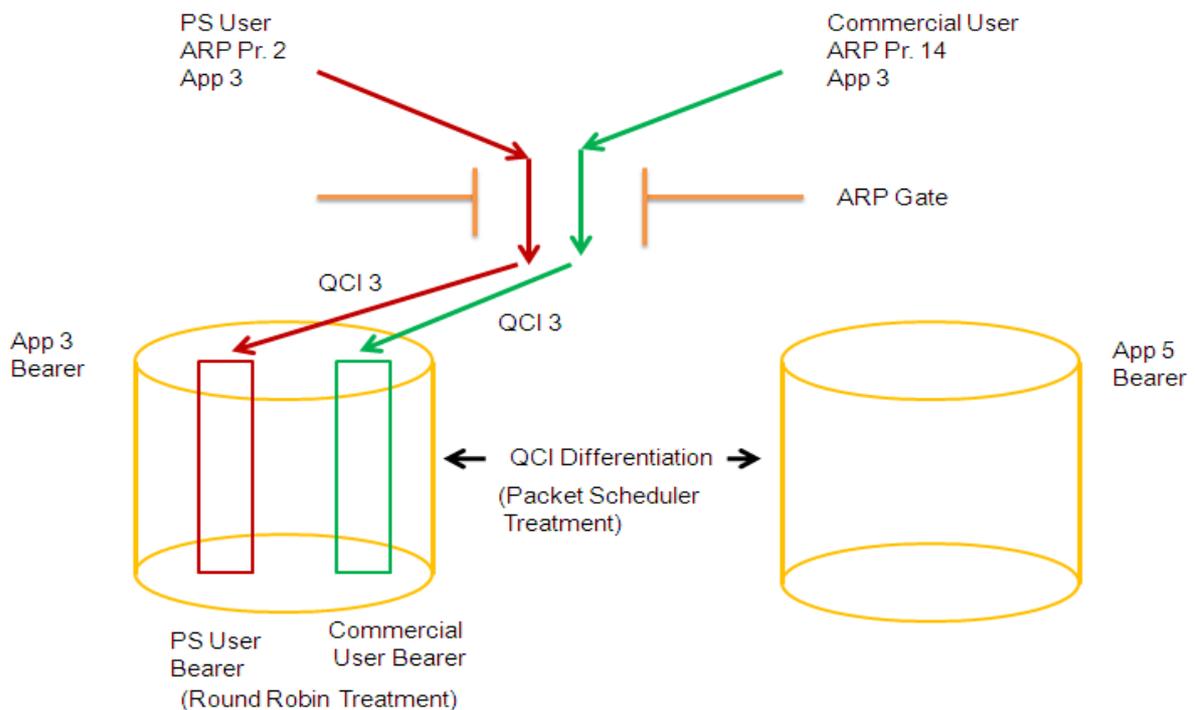


Figure A.5: Bearer Establishment for a Public Safety and a Commercial User in a Non-Congested Situation

Now consider the congested environment situation (see Figure A.6).

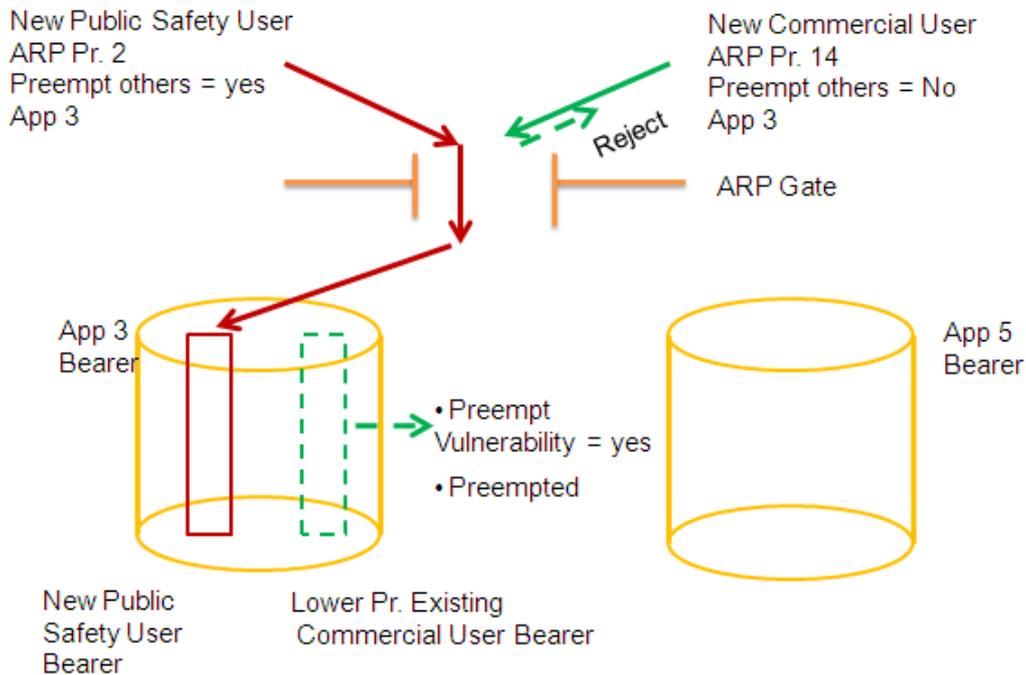


Figure A.6: Bearer Establishment for a Public Safety User in a Congested Network

Since the public safety user has a higher ARP priority, it is considered first for possible bearer assignment within the Application 3 bearer “pipe.” The bearer may be established only for the public safety user and the commercial user request needs to be rejected. The preempt others flag is examined and in this case it is found to be set to “yes.” In order for the public safety user to get a GBR bearer, another lower priority bearer needs to be identified for preemption. In addition, that lower priority bearer needs to have its preempt vulnerability flag previously set to “yes.” If such a bearer exists, that bearer is preempted and the freed resources are applied to the new public safety user. Random selection may be used for preemption in case of a tie of ARP priority values.

A.5 Related Functions

In the illustration of relative priority handling of the public safety user with respect to the commercial user, the focus has been on the priority handling mechanisms. For the public safety user, there are several other aspects of importance including Security [3GPP15], [3GPP10, Sec 4.3.4, Sec. 5.3.10], [3GPP11, Sec. 4.4, Sec. 5.4.3], [3GPP15], [3GPP16, Sec. 14]. Examples of the application of security may entail ciphering/deciphering of data in both the control and the user planes and integrity protection and verification of data in the user plane. Other mechanisms include user identity and equipment confidentiality, entity authentication, and user data and signaling data confidentiality and integrity.

Security Procedures between UE and EPC Network Elements [3GPP15, Sec. 6] include authentication and key agreement, EPS key hierarchy, EPS key identification, and handling of EPS security contexts.

Security procedures between UE and EPC access network elements [3GPP15, Sec. 7] include the mechanism for user identity confidentiality, handling of user-related keys in E-UTRAN, U-Plane security mechanisms, RRC security mechanisms, signaling procedure for periodic local authentication, and also security procedures for both X2 and S1 based HO's.

Appendix B: Shared Network Architectures

B.1 Both RANs Connected to Public Safety EPC Core

Both the PS_eNodeB and the commercial C_eNodeB are connected to the public safety EPC core, as shown in Figure 5.1. Such Radio Network sharing architectures are supported as part of the Multi-Operator Core Network (MOCN) configuration [3GPP10, Sec. 4.3.11] across the S1 interface. The two eNodeBs may run at their respective, distinct carrier frequencies. The commercial RAN is connected to the public safety EPC via the S1 interface for carrying the public safety control and user traffic. C_eNodeB will have both PLMN IDs (based on the selected P-GW) [3GPP2, Sec. 3.2.1]. The public safety user control traffic from the C_eNodeB is carried to the PS_MME [3GPP10, Sec. 4.3.10] via S1-MME interface. The public safety user traffic from the C_eNodeB is carried using the S1-U interface to the PS_S-GW on to PS_P-GW. The PS_UE that has connected to PS_MME can continue to be served by the same MME even when it moves to the C_eNodeB in the same coverage area. It needs to be emphasized that there is overlap between the public safety RAN coverage and the commercial RAN. The public safety RANs form their own public safety network of adjacent cells and the Commercial RANs also form their own commercial network of adjacent cells.

The HO between the PS_eNodeB and the C_eNodeB can be effected in two ways: using the X2 interface between the two eNodeBs, and using the S1 connectivity between the eNodeBs and the PS_MME. The X2 HO is a direct path and hence supports HOs, e.g., needed for data applications which have stringent packet loss requirements. S1 based HO requires uses primarily the PS_MME as a pass through for communications between the two eNodeBs and can be used for streaming video type applications.

In this study, the HO to the commercial RAN using the S1 interface is considered initially. The related mechanisms including the Tracking Area (TA) update without S_GW Change [3GPP10, Sec. 5.3.3.2] and illustrative flowcharts and details for S1 based HO are available in [3GPP10, Sec. 5.5.1.2]

For this architecture of both eNodeBs connected to the PS_EPC, the primary control for public safety users is with the public safety agency, including priority management, user logs, and provisioning. The commercial HSS/AAA need not account for public safety users. All public safety user traffic travels through the PS_EPC even if the public safety user has moved into the C_eNodeB. The S1 traffic bearer between eNodeBs and PS_S-GW is switched from the PS_eNodeB to the commercial C_eNodeB for connecting to the PS_EPC. However, the internal S5 bearer between PS_S-GW and PS_P-GW in the PS_EPC is not affected. Please refer to Figure B.1 for the traffic flow summary.

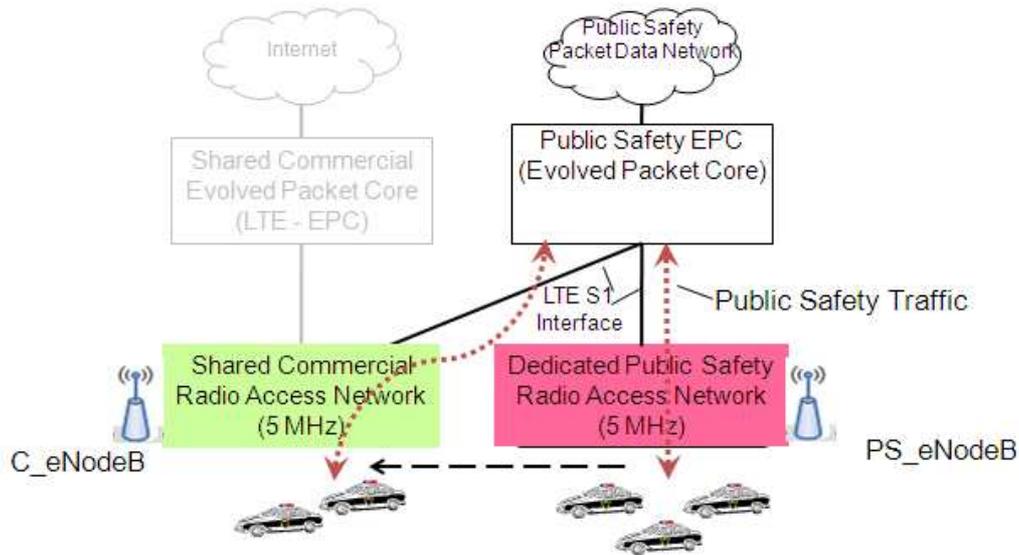


Figure B.1: Separate Network Access Network

Such HO is extensively implemented in the commercially deployed networks including 3G where multiple base stations are connected to a common core (HO between base stations). Hence, considerable experience has been accrued for such an architecture. An illustration of such an intra-MME/S-GW HO flowchart and details are also available in [3GPP16, Sec. 10.1.2] and the extension to inter-frequency HO [3GPP8, Sec. 5.2.4.5], [3GPP16, Sec. 10.1.3.2] has also been covered. Illustrations on how different applications are supported with inter-frequency (and inter RAT) HOs are provided in [3GPP16, Annex E].

B.2 Shared RAN Architecture

In this architectural option, shown in Figure 5.2, the public safety and the commercial traffic are carried through a common RAN but unique traffic paths for the public safety and the commercial traffic exist to the respective EPC cores. The PS_EPC and the C_EPC need to be engineered to carry the respective public safety and the commercial traffic, including during emergency conditions. Such Radio Access Network sharing with n-to-m relationship between RANs and EPC Cores is supported in the LTE/EPC standards [3GPP16, Sec. 10.1.7].

The public safety and the commercial users are provisioned in their respective EPC complexes. The priority management rules for the public safety users are invoked only in the PS_PCRF. The priority order for connection for the UEs is based on their respective public safety and the commercial PLMN IDs [3GPP8, Sec. 5.1]. This architecture allows, potentially, the most optimized use of the total spectrum. It maximizes the revenue/value generation for the total spectrum since any spare capacity can be used by either type of user. The cooperative interfaces between the two EPC's allow committed public safety priority requirements to be met regardless of the public safety or the commercial user loads. The overall scenario is summarized in Figure B.2.

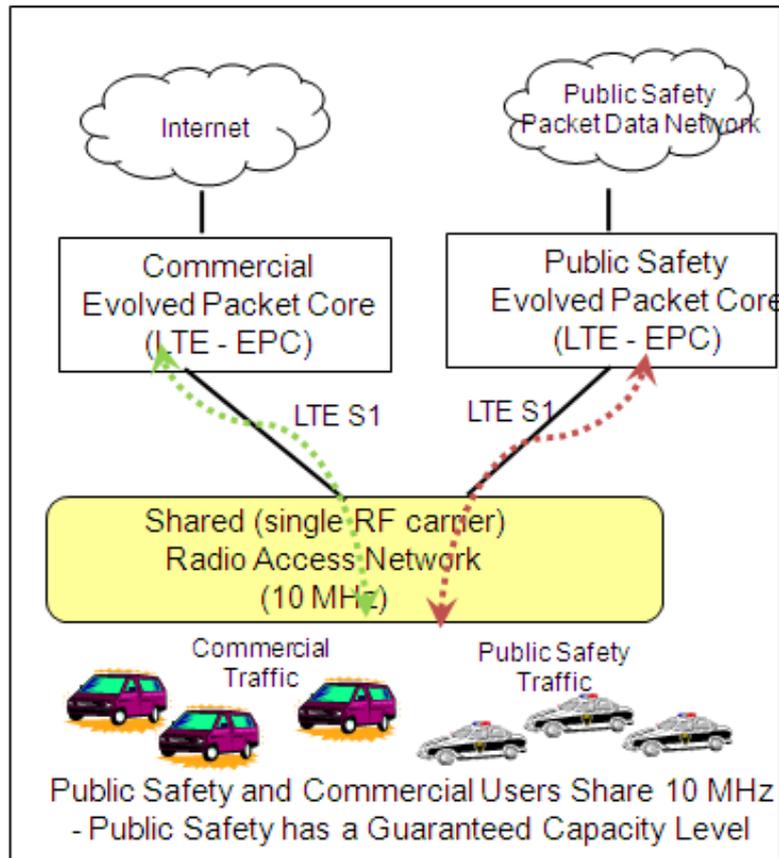


Figure B.2: Shared Radio Access Network

This architecture requires a very tight relationship between the public safety and the shared commercial operator. Major benefit to the public safety community is due to the economies of scale created. The public safety agency as well as the commercial operator have a stake in each other's success. It also allows the commercial operator to manage and operate the total RAN network on behalf of the public safety agency, if desired.

B.3 Independent Public Safety and Commercial Networks

The architecture under consideration is the one shown in Figure 5.3. The public safety user control signaling and traffic is moved from the PS_eNodeB to the C_eNodeB and to the commercial EPC in case of congestion in the public safety RAN. This option relies on considerable involvement by the commercial operator in ensuring the priority treatment for the public safety user when they move over to the commercial RAN. Public safety user can be provided the appropriate priority treatment while in the commercial network. The overall scenario is summarized in Figure B.3.

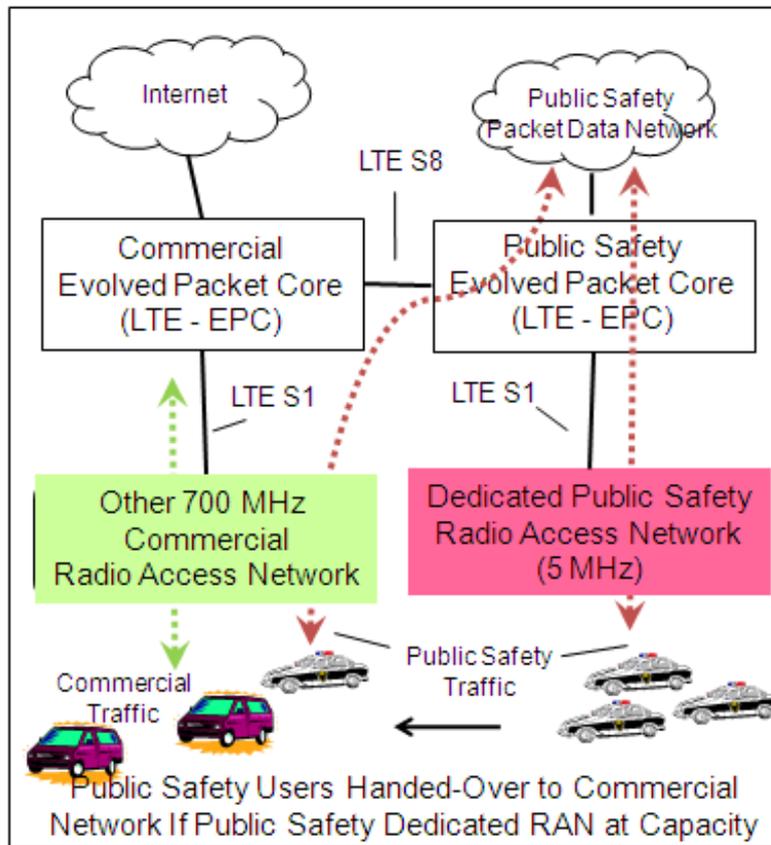


Figure B.3: Separate Radio Access Networks

Each of these three architectures, discussed above, can provide robust, uncompromised priority treatment to the public safety user while in its public safety domain or in the shared commercial domain.

For the initial study, the architecture of separate RANs connected to public safety EPC Core (Figure 5.1) is chosen as a representative architecture since, notionally, it provides independent public safety dedicated RAN and a shared commercial RAN to the public safety user, and always directs the public safety traffic through the public safety core.

The corresponding treatments to ensure public safety users' priority requirements for the other two architectural alternatives are covered in Section 9.

Appendix C: PS_eNodeB and PS_PCRF Activities Summaries

C.1: PS_eNodeB Activities

An illustration of the PS_eNodeB activities is provided in Figure C.1.

RACH, RRC, and initial attach procedures illustration

Broadcast SIB2 to all users (BarringFactor, BarringForEmergency, BarringForSpecial)

public safety users responds for BarringForSpecial due to access classed (12 – 14); implies public safety user

Send Access Success to UE

Receive RRCConnectionRequest with EstablishmentCause (HighPriorityAccess)

Check Establishment Cause

If High Priority

Send RRC Connection Success response to UE #RRC Setup complete

Authentication Procedure

Update Location Procedure

Create Session Procedure

Receive Initial Context Setup Request / Attach Accept (ARP, QCI) from MME

Send RRC Connection Reconfiguration / Attach Accept to UE (QCI)

Return

Else

Send RRC Establishment Failure Response to UE

Return

Figure C.1: eNodeB Procedure Summary for Public Safety user Radio Admission and Initial Attach

C.2 PS_PCRF priority Management

An illustrative procedure summary for the PS_PCRF is indicated in Figure C.2

PS_Priority_Treatment

Check Preempt Others (ARP) Flag

If Yes

 Check Preempt Vulnerability flag for a Lower Priority user

 If Yes

 Invoke Lower Priority Treatment Process ; multiple choices for Preemption

 If lower_bit_rate Treatment acceptable ; e.g., reduced CODEC Rate

 Assign lower bit rate

 Elseif Alternate network available

 Hand over to another network

 Elseif Non-GBR Performance Acceptable

 Convert to N-GBR bearer

 Else

 Detach User ; Need to drop lower priority user

 Send CC Answer to P-GW requesting to set up the bearer # Assign resources to new user

 Return

Else

 Send CC Failure Msg to P-GW to be transmitted to UE ; New User request denied

 Return

Else

; New user cannot preempt others

 Send CC Failure Msg to P-GW to be transmitted to UE ; New User request denied

 Return

Figure C.2: Public Safety User Priority Treatment in the Public Safety Network for Overloads in Both Networks

Appendix D: Public Safety User Scenarios

D.1 New Public Safety User – Public Safety Network not Congested

Figure D.1 provides the summarized view of the admission and bearer establishment for a public safety user. This is based on the illustration of a UE initiated Service Request Procedure available in [3GPP10, Sec. 5.3.4]

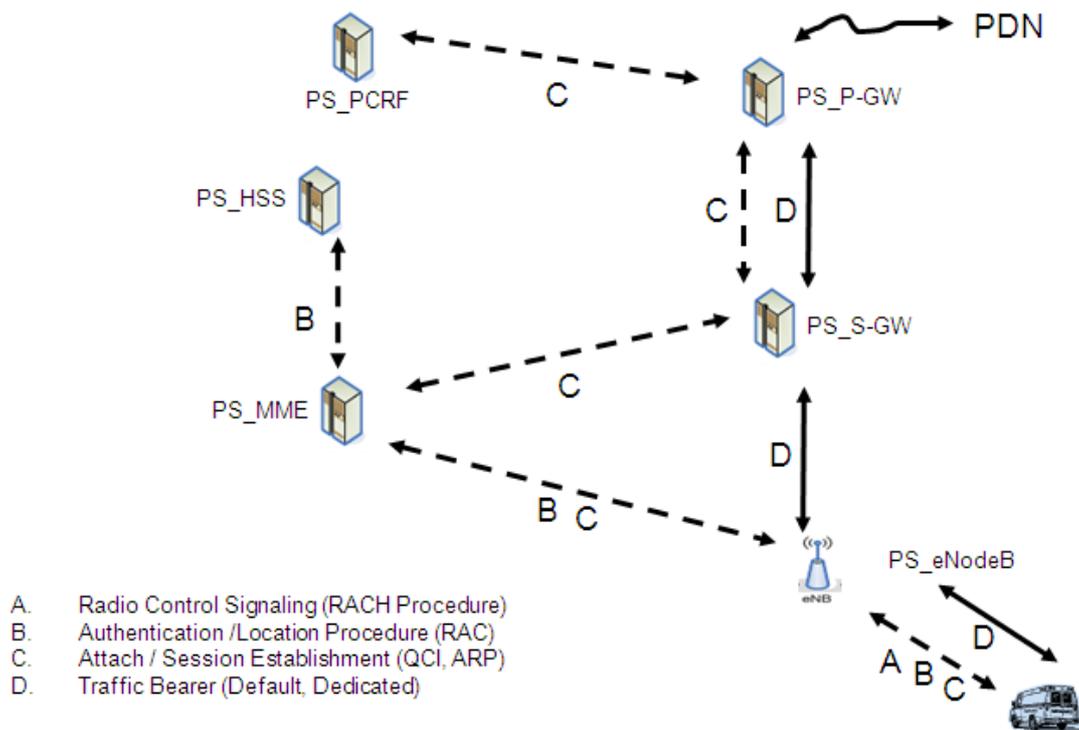


Figure D.1: New Public Safety User in an Unloaded Dedicated Public Safety Network (Summary)

The sequence of major events depicted in Figure D.1 is as follows:

- A. Radio Control Signaling (RACH Procedure): This procedure follows the initial steps for the PS_UE including power on, system acquisition, cell search / PLMN ID, and selection of the public safety RAN as the default for connection. The initial connection is then established.
- B. Authentication / Location Procedure (RAC): These entail the user authentication and authorization followed by retrieval of the bearer attributes (ARP, QCI) from the PS_HSS.
- C. Attach / Session Establishment (QCI, ARP): These are part of establishing a non-GBR or a GBR bearer. The primary control is provided by the PS_PCRF.
- D. Traffic Bearer (default, Dedicated): These bearers, established between the PS_UE, PS_eNodeB, PS_S-GW, and the PS_P-GW, allow the user traffic to flow through.

Figure D.2 provides a set of detailed steps.

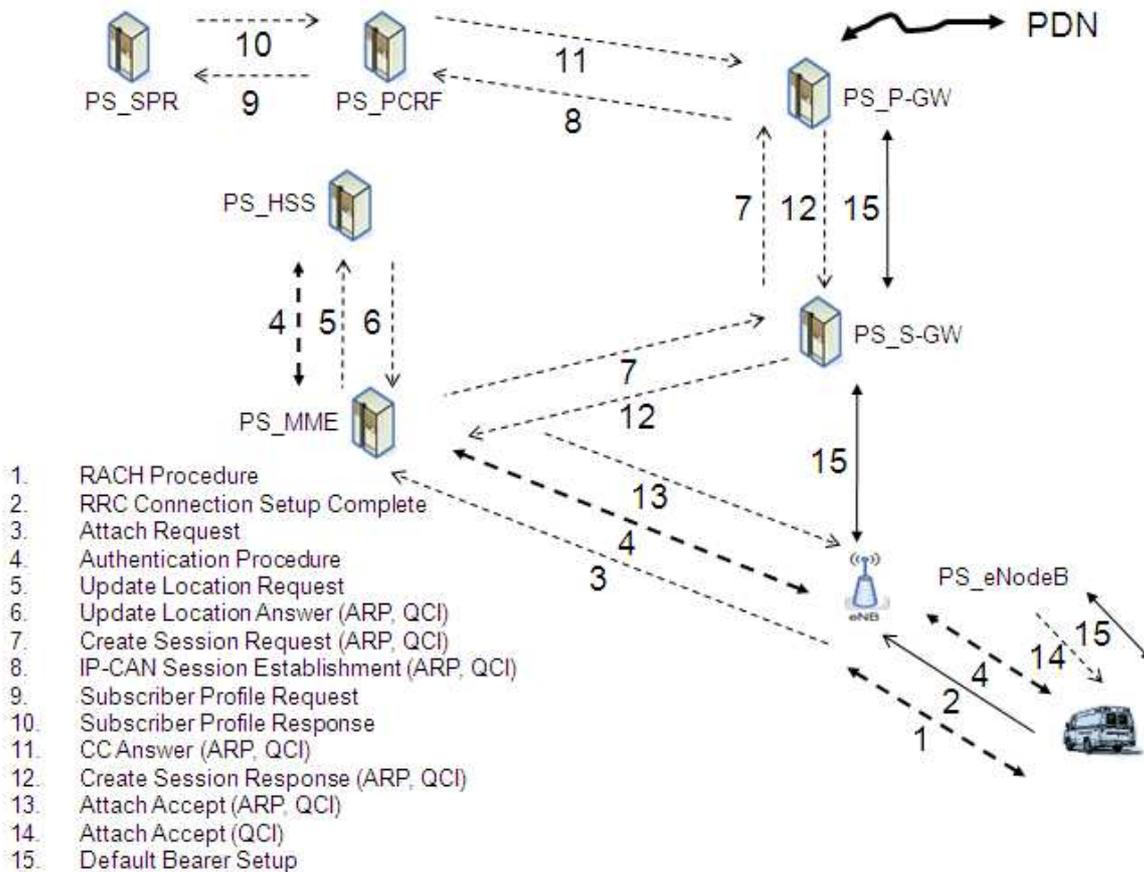


Figure D.2: New PS User in an Unloaded Dedicated Public Safety Network (Key Steps)

1. RACH Procedure: The PS_UE sends a Random access pre-amble (high priority user) to the PS_eNodeB. The PS_eNodeB sends initial uplink grant to the PS_UE
2. RRC Connection Setup complete: The first step in this is availability of radio resources for control and communications. The PS_eNodeB examines the access priority class (12 – 14) and Barring not enabled, and decides to allow the PS_UE radio access. This is followed by the PS_UE sending the RRC request with the Establishment cause (highPriorityAccess). The PS_eNodeB sends the RRC response to the PS_UE.
3. Attach Request: The PS_eNodeB sends attach request with high priority access to PS_MME.
4. Authentication Procedure: The PS_MME initiates the authentication procedure between the HSS and the PS_UE.
5. Update Location request: The PS_MME sends the Update Location request to PS_HSS which retrieves the subscriber data (ARP, QCI).
6. Update Location Answer (ARP, QCI). Upon receiving the Update Location response from PS_HSS, the PS_MME saves the QCI, ARP values in the PS_UE context it maintains.
7. Create Session Request: The PS_MME sends the session request (ARP, QCI) to PS_S-GW which conveys the same to the PS_P-GW.

8. IP-CAN Session Establishment (ARP, QCI): The PS_P-GW assigns the IP address for the PS_UE and sends an IP-CAN establishment request to PS_PCRF.
9. Subscriber Profile Request: PS_PCRF sends a subscriber profile request to the PS_SPR
10. Subscriber Profile Response: The PS_SPR sends the profile response to PS_HSS
11. CC Answer (ARP, QCI): The PS_PCRF invokes the PCC rules and sends the set up bearer request (ARP, QCI) to the PS_P-GW
12. Create Session Response (ARP, QCI): The PS_P-GW sends the create session response (ARP, QCI) to the PS_S-GW which assigns the bearer and sends the message to PS_MME.
13. Attach Accept (ARP, QCI): The PS_MME saves the ARP, QCI values in the PS_UE context and sends the Attach Accept to the PS_eNodeB.
14. Attach Accept (QCI): The PS_eNodeB performs the connection access control procedure and sends the Attach accept (QCI) to the PS_UE.
15. Default Bearer has now been Setup

D.2 New Public Safety User – Public Safety Network Congested, Commercial Network not Congested

Key steps are indicated in Figure D.3.

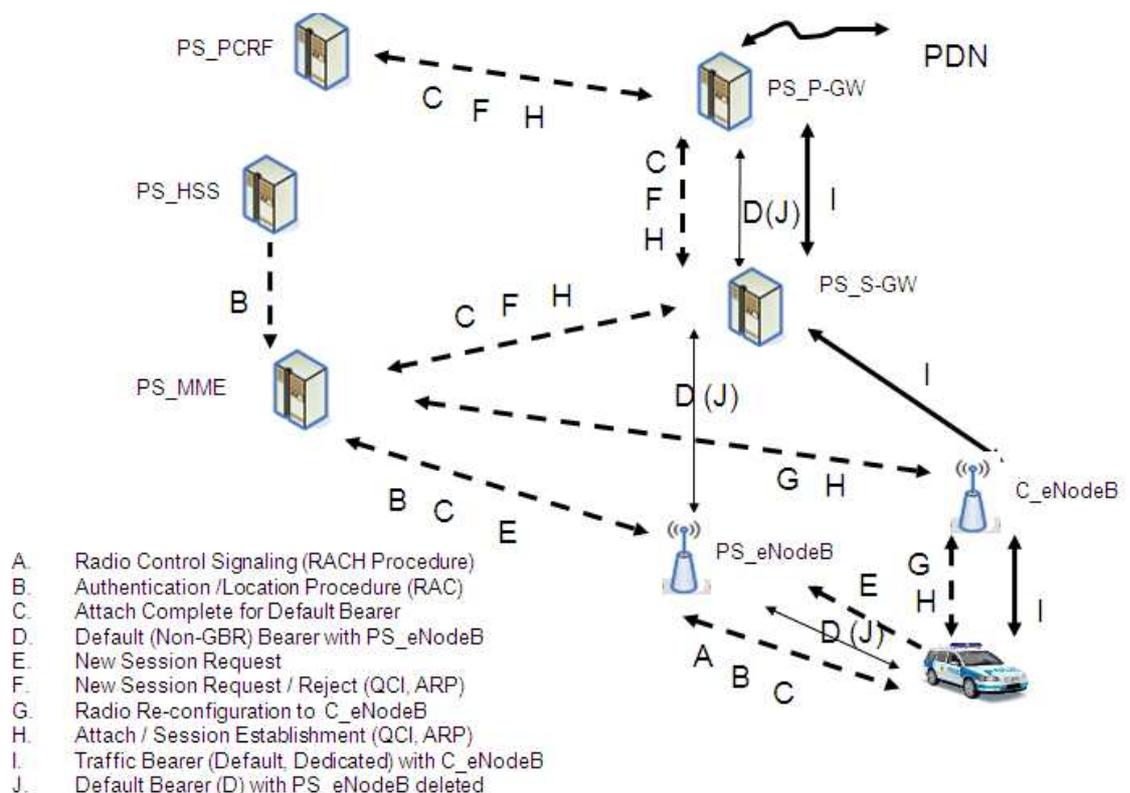


Figure D.3: Public Safety User Moving into the Shared Commercial RAN (Commercial RAN Not Congested)

- A. Radio Control Signaling (RACH procedure): Same as Step #1 in Figure D.2
- B. Authentication / Location Procedure (RAC): Same as Step #2 to #7 in Figure D.2
- C. Attach Complete for Default Bearer: Same as Steps #8 to #14 in Figure D.2
- D. Default (Non-GBR) Bearer with PS_eNodeB: Same as Step #15 in Figure D.2
- E. New Session Request: A modify bearer request is initiated by the PS_UE for additional resources.
- F. New Session Request / Reject (QCI, ARP): The PS_MME's interfaces with the PS_eNodeB, PS_S-GW, PS_P-GW, and PS_PCRF results in rejection of the new bearer request since the PS_eNodeB does not have resources to support the new request.
- G. Radio Re-configuration to C_eNodeB [3GPP16, Sec. 10.2.2.5]: The PS_MME sends a handover request message to the target C_eNodeB and the C_eNodeB sends an HO request acknowledgement. The PS_UE establishes successful RACH and RRC re-configuration procedures with the target eNodeB. To aid in the preferential HO process for the PS_UE, use can be made of non contentions based RACH procedure via use of the high priority RACH preamble by the PS_UE. Upon receiving the HO confirm message from the PS_UE, the C_eNodeB sends a HO Notify message to the PS_MME to indicate successful transfer of the PS_UE to the C_eNodeB.
- H. Attach / Session Establishment (QCI, ARP): The previous steps for creating the bearer (steps #A to #D) are repeated between the PS_EPC and the C_eNodeB.
- I. Traffic Bearer (Default, Dedicated) with C_eNodeB: The above procedures allow the public safety user traffic to be supported by the C_eNodeB.
- J. Default Bearer (D) with PS_eNodeB deleted: This involves the PS_MME sending the UE Context command to PS_eNodeB and PS_eNodeB sending the response back to PS-MME.

It may be noted that the primary message in the case of default bearer is "Create Session Request" whereas for dedicated bearer is "Create Bearer Request"

D.3 New Public Safety User – Both the Public Safety and Shared Networks Congested

A representative scenario is provided in Figure D.4.

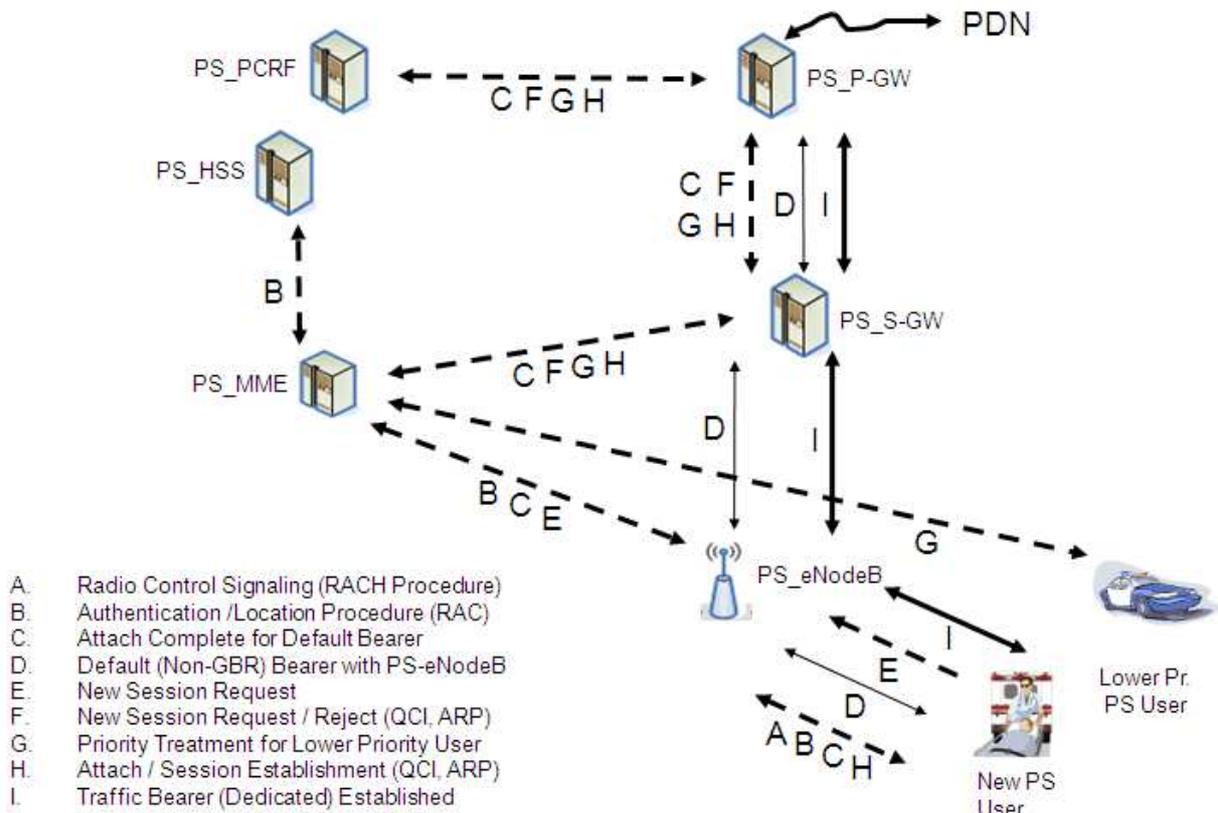


Figure D.4: New Public Safety User in a Congested Public Safety Network – Priority Treatment

- A. Radio Control Signaling (RACH Procedure): Same as Step #A in Figure 6.4
- B. Authentication / Location Procedure (RAC): Same as Step #B in Figure 6.4
- C. Attach Complete for Default Bearer: Same as Steps #C in Figure 6.4
- D. Default (Non)GBR) Bearer with PS_eNodeB: Same as Step #D in Figure 6.4
- E. New Session Request: Same as Step #E in Figure 6.4
- F. New Session Request / Reject (QCI, ARP): Similar to Step #F in Figure 6.4. In addition to an indication from the PS-eNodeB, the PS_MME also gets failure message from the C_eNodeB. Note that the source eNodeB and the UE keep some context information to enable return of UE in case of HO failure [3GPP16, Sec. 10.1.2.1].
- G. Priority Treatment for Lower Priority User: This step now entails identification of a lower priority public safety user to be preempted. The PS_MME sends the E-RAB command to the PS_eNodeB which in turn carries out the radio bearer release (RRC procedure) with the lower priority PS_UE. It then sends the E-RAB release response to PS_MME.
- H. Attach / Session Establishment (QCI, ARP): Same as Step #H in Figure 6.4 except it is with the PS_eNodeB.
- I. Traffic Bearer (Dedicated) Established: Same as Step #H in Figure 6.4 except it is with the PS_eNodeB.

D.4 Public Safety User in Shared Network – Hand Back to Public Safety Network

This section covers the scenario of the handing back of a public safety user from the C_eNodeB to the PS_eNodeB upon availability of resources in the PS_eNodeB as discussed in Section 6.7. The major steps are shown in Figure D.5.

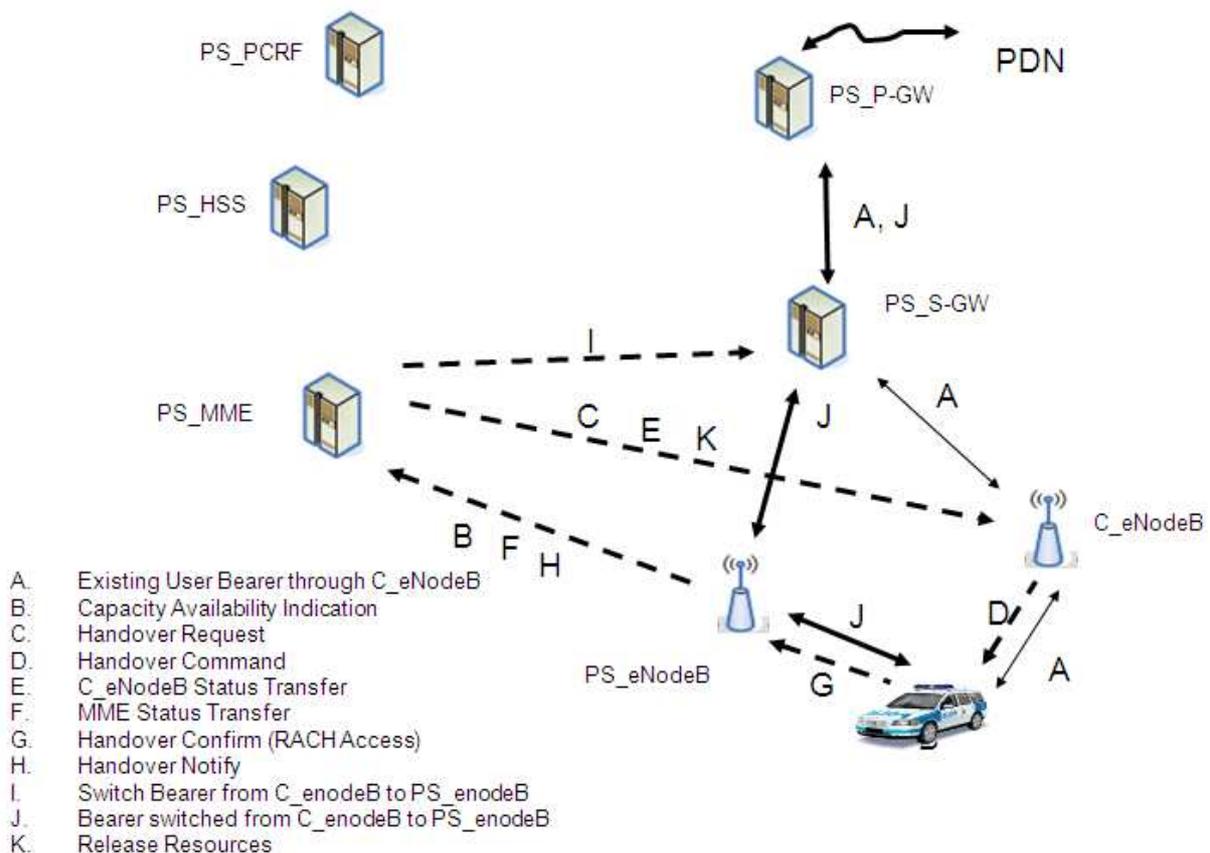


Figure D.5: Public Safety User in Shared Network – Hand Back to Public Safety Network

- A. The initial condition pertains to the existence of a bearer for the PS_UE via the C_eNodeB and PS_S-GW and PS_P-GW.
- B. Upon availability of freed up resources, the PS_eNodeB signals the PS_MME for a possible move of a PS_UE from the C_eNodeB to the public safety RAN.
- C. The MME sends a HO command to the C_eNodeB
- D. The C_eNodeB identifies a PS_UE to be moved to the public safety RAN. It sends the HO command to the chosen PS_UE.

- E. The source C_eNodeB transfers the PDCP context to the PS_MME. The C_eNodeB also forwards the data stored in the PDCP buffer to the target PS-eNodeB via PS-S-GW.
- F. The MME sends the US context to the target PS_enodeB.
- G. The PS_UE performs the various RAN-related procedures needed for HO including accessing the target PS_eNodeB using the RACH procedure. Once the status and data have been transferred to the target PS_eNodeB and the UE is able to establish a RAB on the target PS_enodeB, it sends the HO confirm message to the target PS_enodeB.
- H. When the target PS_eNodeB receives the HO confirm message, it sends a HO notify message to the PS_MME.
- I. The PS_MME requests the PS_S-GW to switch the public safety user bearer from the source C_eNodeB to the target PS_eNodeB.
- J. The EPS/RB bearer is now established between the PS_UE and the PS_P-GW via the PS_eNodeB and the PS_S-GW.
- K. The PS_MME then informs the source C-eNodeB to release the resources originally used by the PS_UE

Appendix E: Alternative Shared Commercial Architectures

E.1 Shared RAN Architecture

In reference to the architecture shown in Figure 5.2,, all eNodeBs are identical whether considered to be owned by the public safety agency (PS_eNodeB) or the commercial operator (C_eNodeB). They operate over the total 10 MHz spectrum. Each eNodeB is connected to both the PS_EPC and the C_EPC through the S1 interface. Each eNodeB has its own distinct coverage area and the HO between eNodeBs will be the standard HO as is applicable for adjacent cells in commercial deployments. Each eNodeB has the same attributes, parameters, and application logic so that identical treatment is provided by each eNodeB. From network management and ownership viewpoint, the public safety agency and the commercial operator may need to decide on who owns which eNodeB, PS_enodeB, and C_eNodeB as appropriate. The network management for the eNodeBs will be done through the respective OA&M consoles.

Both the PS_UEs and C_UEs operate over the total 10 MHz spectrum. The distinction is based on their subscriber IDs being populated in the respective PS_HSS and C_HSS. They store the respective Home PLMN ID's. The "opposite" PLMN ID will be in their "forbidden" PLMN ID list so that public safety user cannot interface with the C_EPC and the commercial user cannot interface with PS_EPC

The PS_UE and the C_UE connects to the available eNodeB with the strongest signal strength. Each eNodeB supports traffic from both the PS_UE and the C_UE. The eNodeB directs the control and user traffic from the PS_UE and C_UE to PS_EPC and C_EPC respectively.

Similar to the discussion for the previous architectural alternative, the focus of the priority management is on the RB Assignment. Each EPC and the S1 backhaul will be engineered sufficiently to carry the respective traffic for the public safety and the commercial users.

A PS_UE or the C_UE will go through the standard steps for radio communications, radio resource assignment, and radio bearer establishment.

The startup process starts when a user powers on and initiates radio communication RACH procedure with the eNodeB. PS_UE will always be guaranteed radio connection (RACH). On the other hand for commercial user in congested mode, communication may not be established.

Similarly, for radio resources, the RRC treatment is provided based on the HighPriorityAccess field for public safety users.

The assignment of the bearer will be based on the priority structure as defined for the public safety and the commercial users. In this shared environment like before, a PS_max_capacity allocation limit may be agreed to between the public safety agency and the commercial operator. The bearer assignment can be done in the framework of this maximum allocated capacity for the public safety users in the shared RAN environment.

The notion of public safety capacity allocation is summarized in Figure E.1.

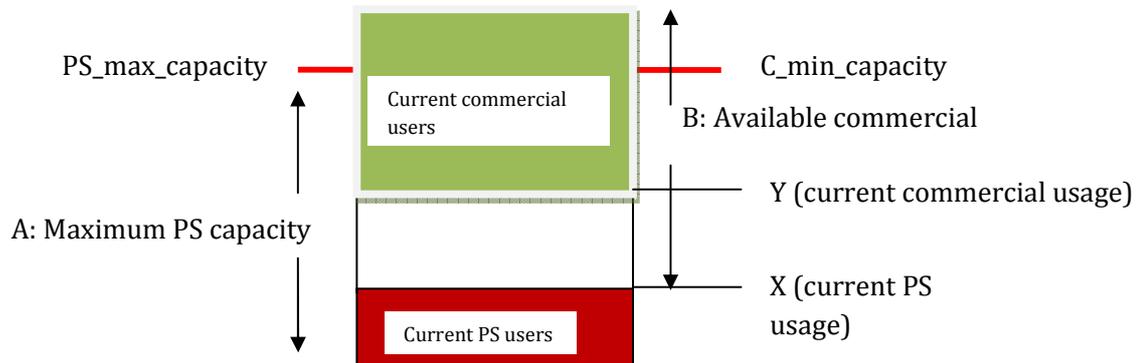


Figure E.1: Available capacity for Public Safety and Commercial users

The public safety users will have access to the capacity up to the allocated value. In this range, the public safety users will always get higher priority treatment in case of the presence of the commercial users. If the PS_max_capacity is set to 100%, then the complete bandwidth capacity of the eNodeB can be used by the public safety users by invoking the priority mechanisms. This implies the co-existence of the public safety and commercial users across the whole capacity domain. For capacity management, the limit parameter PS_max_capacity is provisioned into each eNodeB to reflect the maximum capacity available to the public safety users. The remaining capacity value C_min_capacity (Total – PS_max_capacity) indicates the minimum capacity available to the commercial users.

In case the public safety users are not using their allocated capacity, the commercial users will be able to use the “spare” capacity in addition to the guaranteed capacity they are entitled to.

The capacity available in the eNodeB from the public safety user perspective is the capacity “A” shown in Figure 9.1. The capacity available in the same eNodeB from the commercial user perspective is the capacity “B” which can vary dynamically.

The priority treatment for the public safety users, especially in the shared region, will basically be the same as discussed in the case of the Architecture 1 wherein the commercial RAN was connected to the PS_EPC.

In order to maximize the usage of the scarce spectrum resources, while at the same time meet the priority requirements of the public safety users in their allocated domain, the dynamic values X and Y are available to eNodeB. The eNodeB has the value of PS_max_capacity (or C_min_capacity) and the dynamic values of X and Y to take decision for public safety and commercial users.

Figure E.2 summarizes the data available to the eNodeB for load management. The eNodeB has the provisioned information about the PS_max_capacity associated with the public safety and subtracting this value from the total eNodeB capacity (say normalized to 1) provides the C_min_capacity for the commercial users in its domain. X and Y correspond to the current usage of the public safety and the commercial users respectively. Clearly, the range for X is from zero to

PS_max_capacity and the range of Y is from zero to the total capacity of the eNodeB. For a given value of X and Y, the remaining capacity available for the public safety user is (PS_max_capacity - X) and for the commercial users is ((1 - Y) - X).

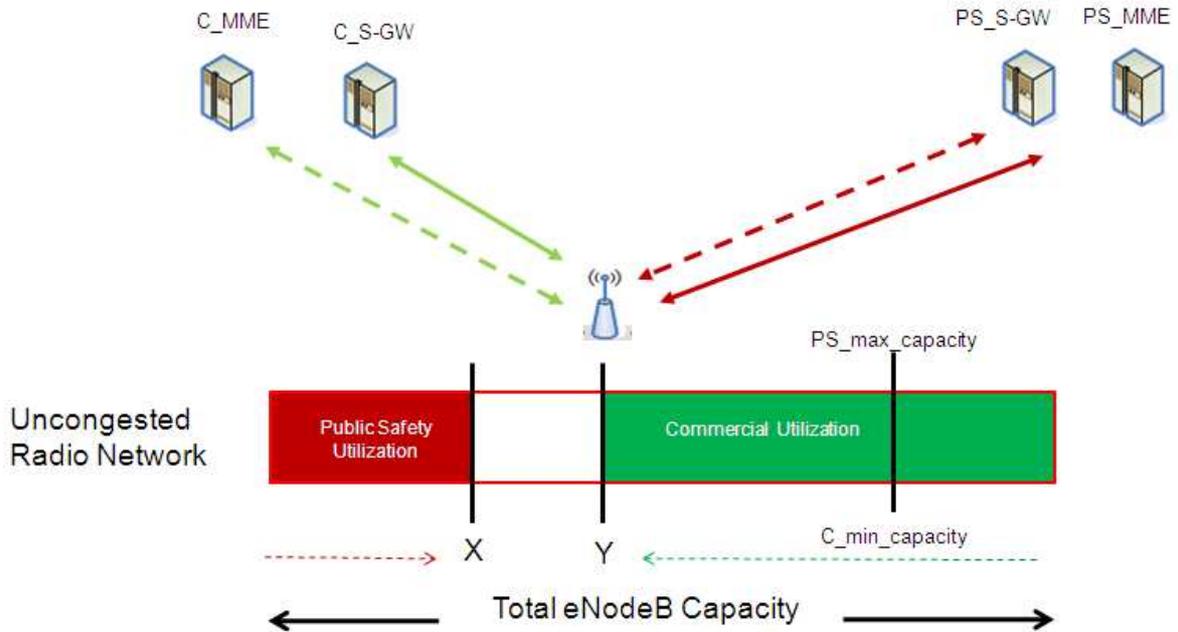


Figure E.2: Capacity Data for MME Load Decision

The entities and interfaces involved in managing the public safety and the commercial users are indicated in Figure E.3.

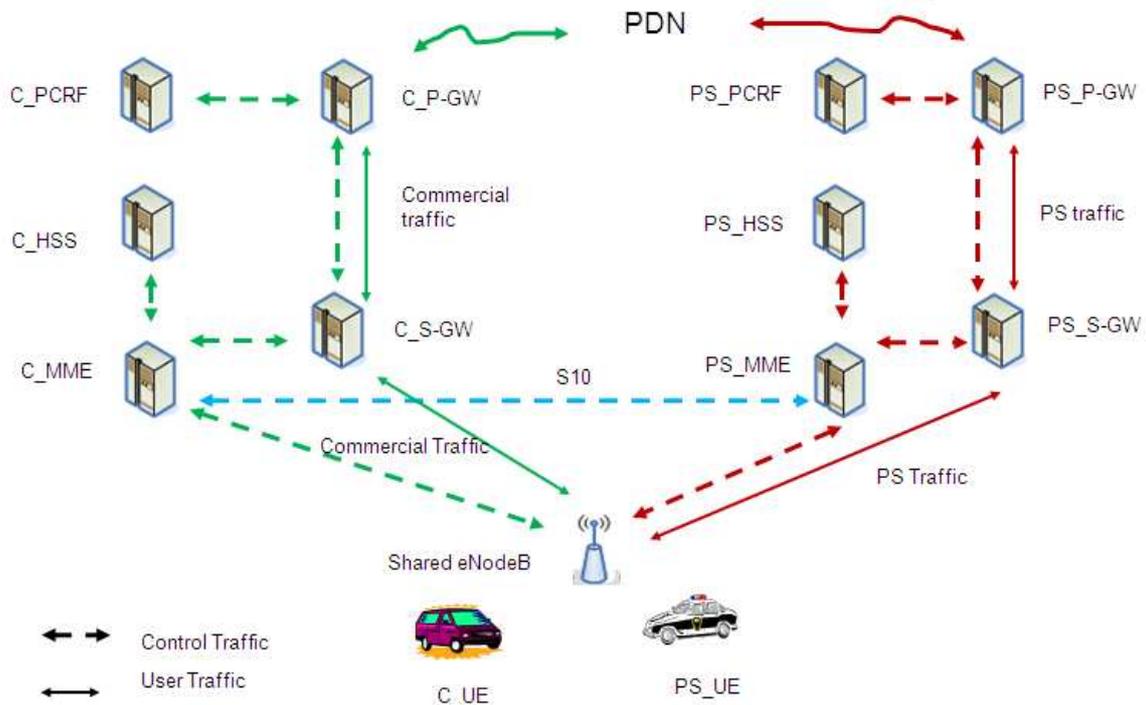


Figure E.3: Shared RAN Public Safety and Commercial Traffic Management

The following provides the usage of the load data and the process for load management in the shared environment where the public safety user gets priority treatment in the shared space.

Consider the following scenarios.

a) $X < PS_max_capacity$ and $Y < C_min_capacity$

There is spare capacity for both the public safety and the commercial users. The eNodeB will assign resources to the public safety and commercial users appropriately.

b) X is not equal to Y (and $Y > C_min_capacity$)

In this case, public safety users are using only partial capacity allocated to them and the commercial users can use the remaining available spare capacity.

In case a new public safety user comes in, eNodeB knows that unused capacity is still available to the public safety users $((1 - Y) - X)$. Again in this case, priority preemption is not needed and a new public safety user can be allocated the necessary resources.

Also, if a new commercial user comes in, eNodeB knows that spare capacity is available to a new commercial user and allocates the resources accordingly.

c) X is equal to Y $((1 - Y) > C_min_capacity)$

Here, the commercial users have used all the spare capacity which was available in the public safety allocated space. No capacity is available for the new commercial users but public safety user may preempt a commercial user since commercial users are using part of the public safety allocated capacity. The situation is summarized in Figure E.4.

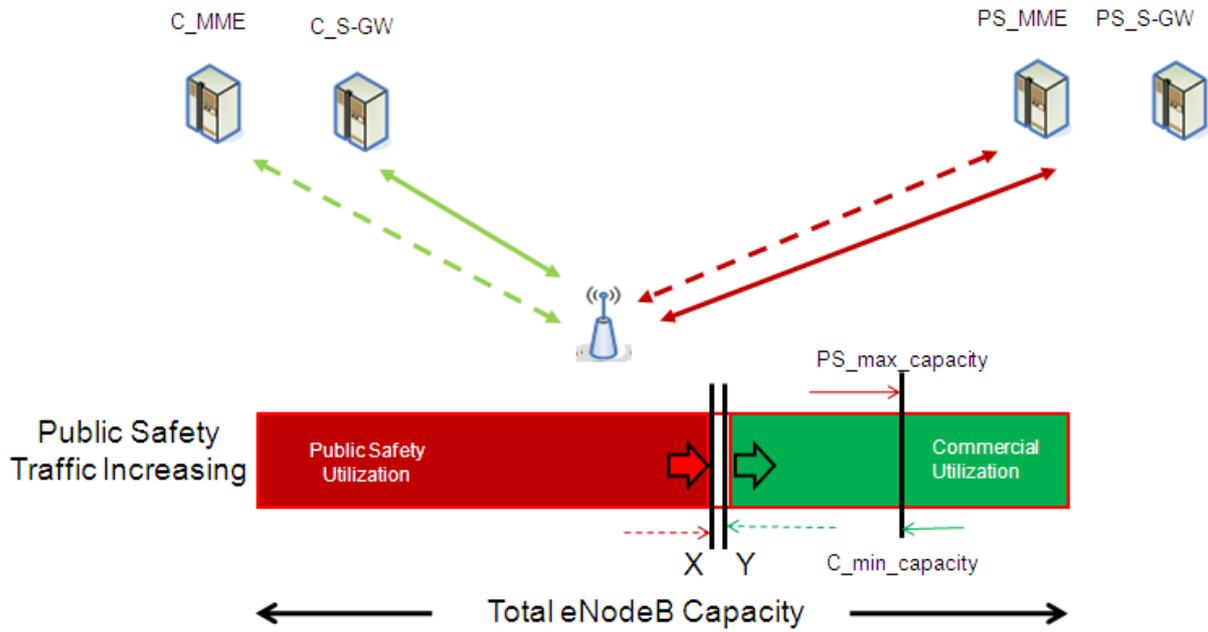


Figure E.4: Load Management in Shared RAN – Preemption of Commercial User

If a new public safety user comes in, the eNodeB knows that the commercial user is using the public safety allocated capacity ($X < PS_max_capacity$). The C_MME works with the eNodeB to preempt a commercial user. The eNodeB then assigns the necessary resources to the new public safety user. X will get incremented and Y will get correspondingly decremented. This will continue until X reaches PS_max_capacity and Y reaches C_min_capacity

However if a new commercial user comes in, no resources can be assigned to the commercial user ($X = (1 - Y)$) and the new commercial user is not allowed to get a bearer.

d) $X = PS_max_capacity$ and $Y = C_min_capacity$

In this case, both the public safety and the commercial users are using full capacity in their respective domains and there are no resources available in the eNodeB for either type of user. This situation is depicted in Figure E.5.

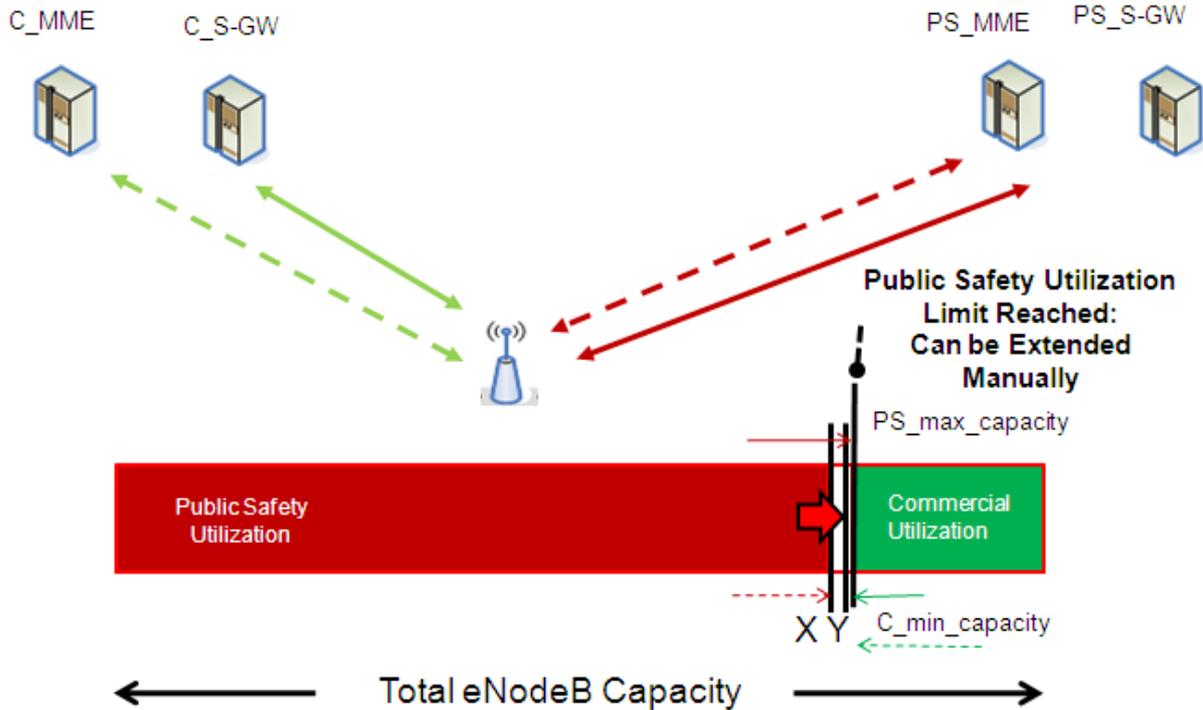


Figure E.5: Public Safety Users at Their Capacity Limit – Priority Treatment within Public Safety Community

If a new public safety user comes in, the eNodeB, along with PS_MME, invoke the priority mechanism within the public safety community and preempt a lower-priority public safety user to free up resources for the new public safety user.

For a new commercial user, no resources can be assigned to the commercial user and the new commercial user is not allowed to get a bearer by eNodeB and C_MME.

E.2 Independent Public Safety and Commercial Network Architecture

This refers to the architecture in Figure 5.3. While the public safety user is in the commercial network, two major scenarios can be supported as mentioned in Section 3.

The Home Routed traffic propagation approach entails the public safety traffic being routed via the C_S-GW and the PS_P-GW (see Figure E.6).

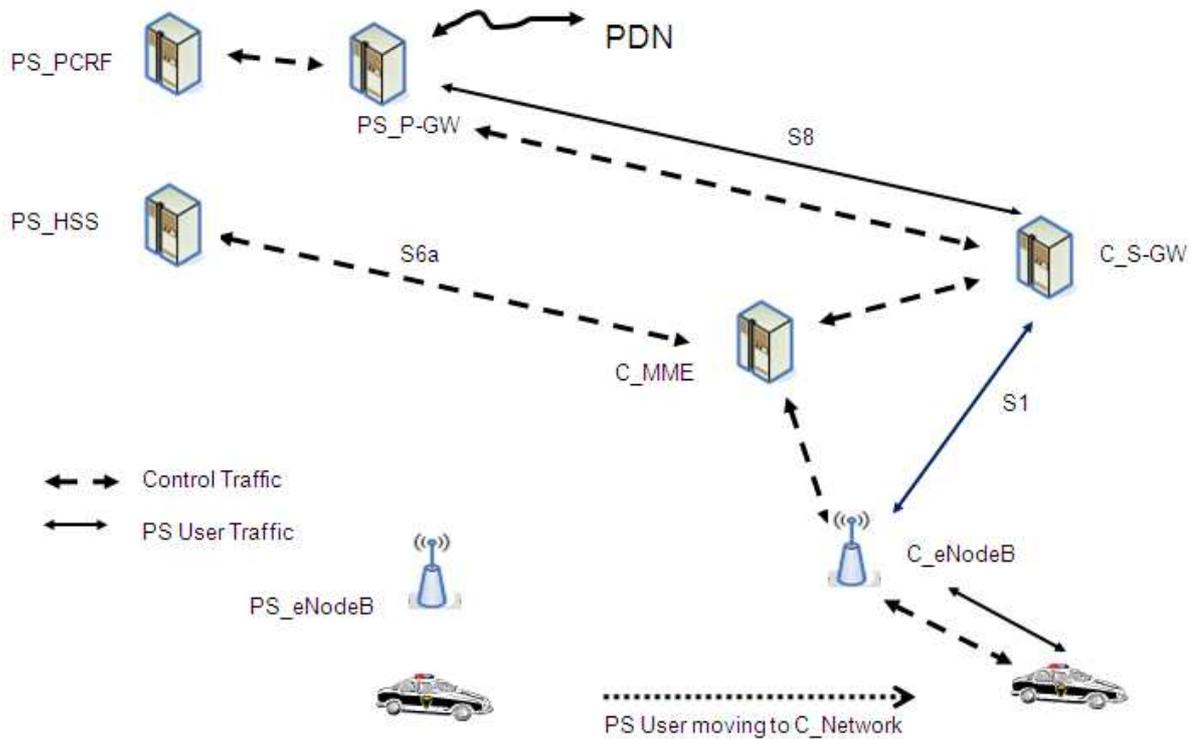


Figure E.6: Home Routed Scenario for Public Safety user in the Shared Commercial Network

The S6a and the S8 interfaces between the commercial and the public safety networks are utilized. The commercial C_eNodeB has both the PS_PLMN ID and the C_PLMN ID stored. The EPC path between the C_S-GW and the C_P-GW is insulated from the public safety user traffic. The PS_PCRF is still involved in managing the public safety users. S8 bearer path between the C_S-GW and the PS_P-GW are used for public safety traffic.

Local Breakout is the other standards supported approach wherein the public safety traffic is routed through the commercial core (C_S-GW and C_P-GW) (see Figure E.7)

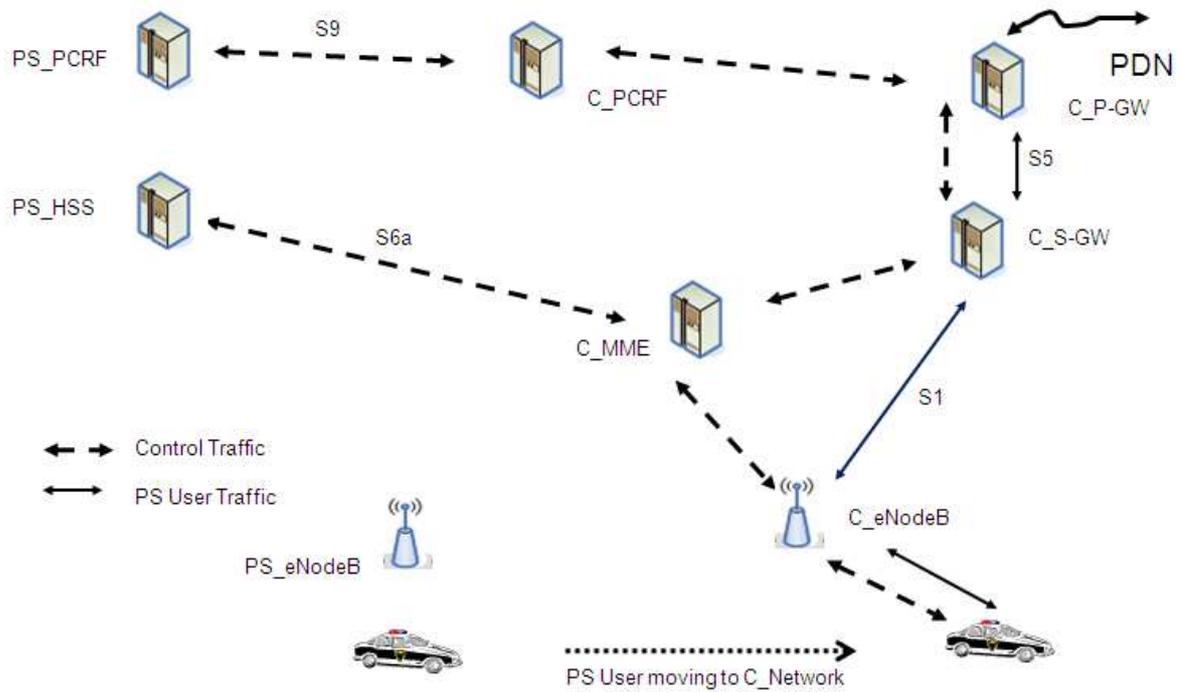


Figure E.7: Local Breakout Scenario for Public Safety User in the Shared Commercial Network

The S6a and the S9 interfaces between the commercial and the public safety networks are used. The C_PCRF gets the public safety treatment rules from the PS_PCRF. The commercial C_eNodeB has only the C_PLMN ID stored. The EPC S5 bearer in the commercial core has to carry both the public safety and the commercial user traffic.

Appendix F: Public Safety User Roaming

For a roaming public safety user into a visitor public safety network, as a preference, it is proposed that the Local Breakout [3GPP9, Sec 5] be applied in such cases since the public safety users may need to work as a “group.” For such situations, the Local Breakout traffic for the members of the group stays within the visiting public safety network. The Local Breakout scenario is similar to the one in Figure E.7 and some of the key steps are identified in Figure F.1 [3GPP10, Fig. 4.2.2-2]. The V_PS_PCRF [3GPP9, Sec. 6.2.1.3] works with the H_PS_PCRF [3GPP9, Sec. 6.2.1.4] to provide the priority treatment for the public safety user in the visitor network.

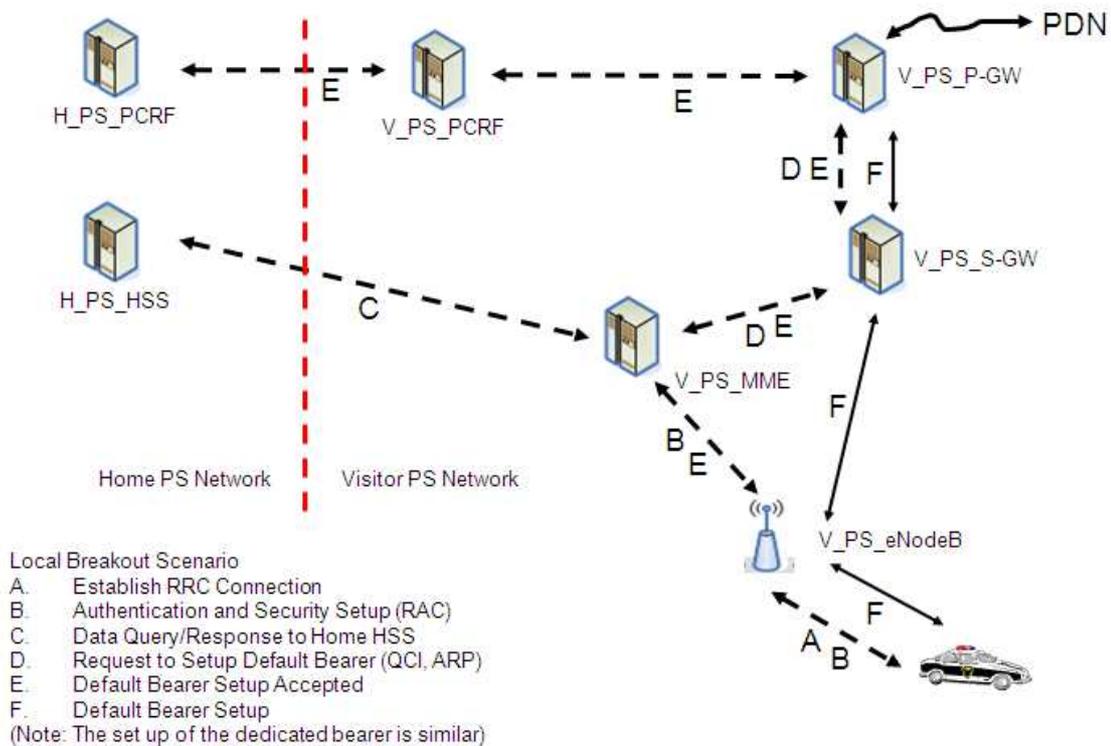


Figure F.1: Public Safety User Roaming into a Visitor Public Safety Network (Local Breakout)

However, when instead of roaming into a public safety network, the public safety user roams into another visitor 700 MHz commercial LTE network, then the Home Routed Scenario [3GPP9, Sec. 5.2] is preferred since it focuses on sending the public safety traffic through the public safety home core (See Figure F.2) [3GPP10, Fig. 4.2.2-1]. The home H_PS_PCRF still provides the priority treatment rules for the public safety user while roaming in the commercial LTE network since the visitor V_C_P-GW gets its priority direction from the home H_PS_PCRF. The PS UE needs to support dual/multi frequency modes.

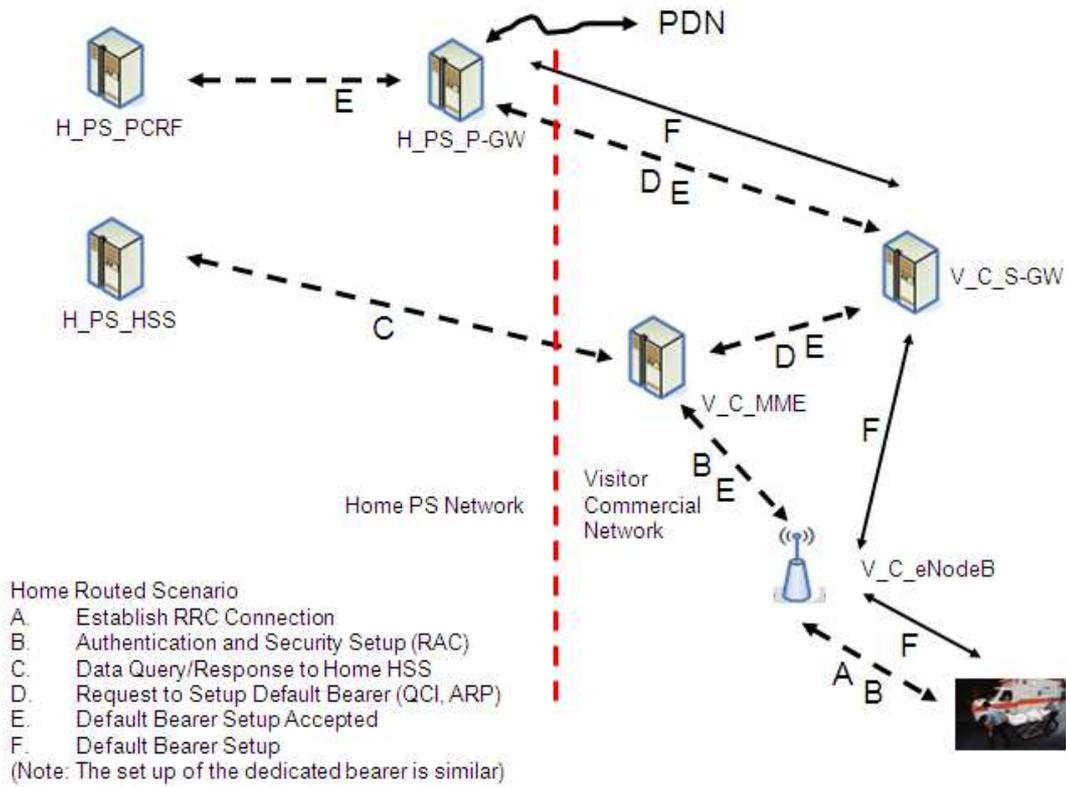


Figure F.2: Public Safety User roaming into a Visitor LTE Based Commercial Network (Home Directed)

Appendix G: X2 Interface Based Data Application Hand Over (HO)

The HO for the architecture in Figure 5.1 can be done by deploying and using the X2 connectivity between the PS_eNodeB and the C_eNodeB [3GPP16, Sec. 20]. It supports inter-frequency handovers between two different eNodeBs [3GPP16, Sec. 22.3.4] (see Figure G.1)

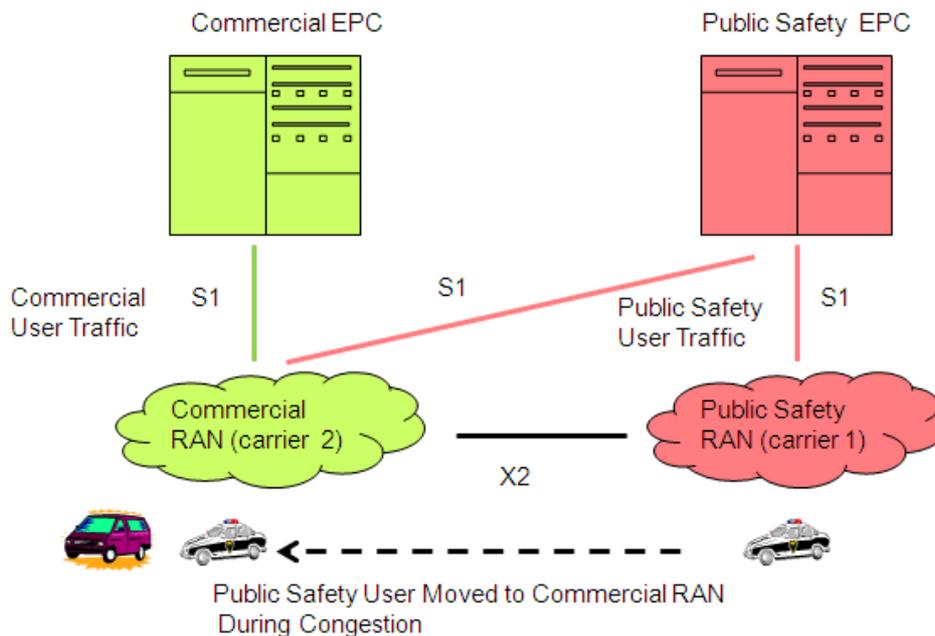


Figure G.1: X2 Based Hand Over (HO)

The HO Control signaling process is the same as before. Appendix A provides a summary of the X2 based HO. However, in order to maintain the integrity of the data stream to the user, there should not be a discontinuity in the packet flow from the public safety user viewpoint.

The overall scenario is indicated in Figure G.2. During transition of the public safety user from the public safety RAN to the Commercial RAN, the PS_S-GW sends the data to the source PS_eNodeB until the path switch command to start sending the data to the target C_eNodeB [3GPP16, Sec. 20]. The PS_eNodeB sends the received user traffic to the target C_eNodeB across the X2-U interface. The target C_eNodeB buffers the data and maintains the data until it receives the subsequent user traffic data from the S-GW. The target eNodeB sends the buffered data prior to sending the direct path data to the UE. This keeps data received by the UE consistent.

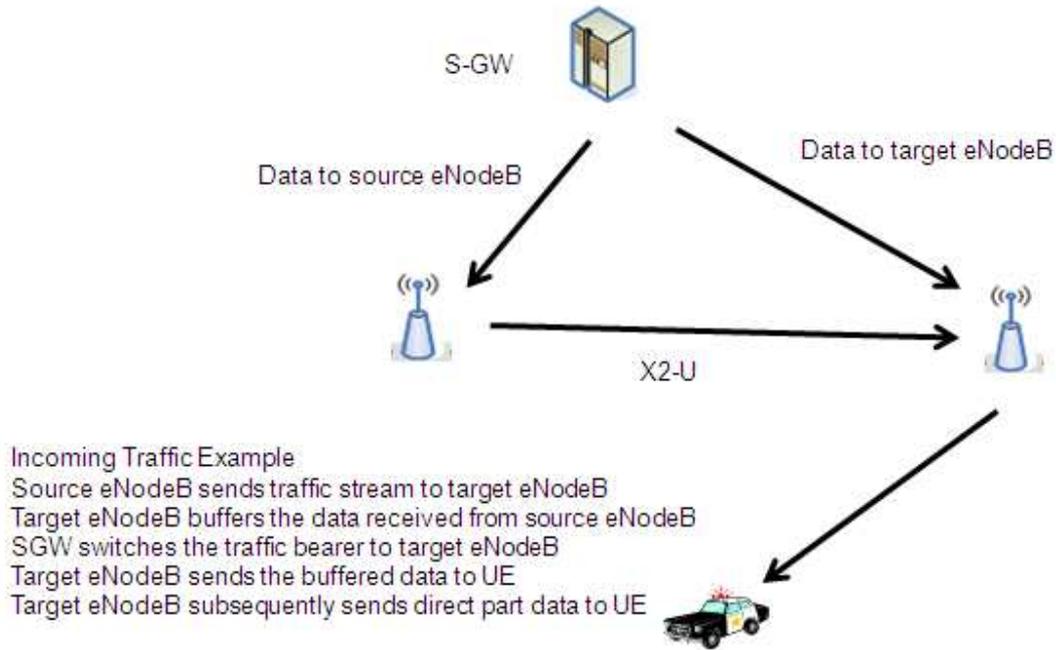


Figure G.2: User Data Traffic Continuity for UE

X2 based HO flowchart and details are available in Figure A.2 [3GPP10, Sec. 5.5.1.1].

Appendix H: Company Profile

Profile: Roberson and Associates, LLC

Roberson and Associates, LLC, is a technology and management consulting company with government and commercial customers that provides services in the areas of RF spectrum management, RF measurements and analysis, and technology management. The organization was founded in 2008 and is composed of a group of select individuals with corporate and academic backgrounds from Motorola, Bell Labs, IITRI (now Alion), independent consulting firms, and the Illinois Institute of Technology. Together the organization has over 200 years of the high technology management and technical leadership experience with a strong telecommunications focus.

Profiles: Roberson and Associates, LLC, Staff

Dennis A. Roberson, President and CEO, Roberson and Associates

Mr. Roberson founded Roberson and Associates in 2008, and is concurrently Vice Provost and Research Professor in Computer Science at the Illinois Institute of Technology in Chicago, Illinois. He assists with IIT's technology transfer efforts, the development of new research centers, and technology-based business ventures. Professor Roberson is an active researcher in the wireless networking arena and is a co-founder of IIT's Wireless Network and Communications Research Center (WiNCom). His specific research focus areas include dynamic spectrum access networks, spectrum occupancy, spectrum management, and wireless interference and its mitigation. He currently serves on the governing or advisory boards of several technology-based companies, including four in the telecommunications industry. Prior to IIT, he was EVP and CTO at Motorola. While in this role, he served on the FCC Technology Advisory Committee (TAC). Professor Roberson has had an extensive corporate career including major business and technology responsibilities at IBM, DEC (now part of HP), AT&T, and NCR. Professor Roberson has BS degrees in Electrical Engineering and in Physics from Washington State University and a MSEE degree from Stanford.

Kenneth J. Zdunek, Ph.D. V.P. and Chief Technology Officer

Dr. Zdunek is Vice President and the Chief Technology Officer of Roberson and Associates. He has 35 years of experience in wireless communications and public safety systems. Concurrently he is a research faculty member in Electrical Engineering at the Illinois Institute of Technology, in Chicago, Illinois, where he conducts research in the area of dynamic spectrum access and efficient spectrum utilization, and teaches a graduate course in wireless communication system design. He is a Fellow of the IEEE, recognized for his leadership in integrating voice and data in wireless networks. Prior to joining Roberson and Associates, he was VP of Networks Research at Motorola, a position he held for 9 years. Dr. Zdunek was awarded Motorola's patent of the year award in 2002 for a voice-data integration approach that is licensed and extensively used in GSM GPRS. He holds 17 other patents, included patents used in public safety trunked systems and cellular and trunked systems roaming. He directed the invention and validation of Nextel's iDEN™ voice-data air interface and IP based roaming approach, and was the principal architect of Motorola's SmartNet™ public safety trunking protocol suite. In the 1990's, he directed a Spectrum Utilization and Public Safety Spectrum Needs Projection submitted to the FCC in support of the 700 MHz spectrum allocation for Public Safety. He

was awarded the BSEE and MSEE degrees from Northwestern University, and the Ph.D. EE degree from the Illinois Institute of Technology. He is a registered Professional Engineer in the State of Illinois.

Suresh R. Borkar, Ph.D. Senior Principal Investigator

Dr. Borkar is a Senior Principal Investigator at Roberson and Associates and a member of the faculty in the Electrical and Computer Engineering (ECE) department at the Illinois Institute of Technology (IIT), Chicago. Previously, he was with AT&T/Lucent Technologies/Alcatel-Lucent (ALU) for over 26 years responsible for various facets of product management, systems engineering, architecture, development, integration and testing, and customer management in Computer and Networking systems, Wireline Switching systems, Data systems, and Wireless systems. He was the Director for Customer Management for 3G mobility systems responsible for customer positioning, acceptance, and revenue realization. He was previously the Chief Technology Officer (CTO) and Managing Director, Lucent India Inc., responsible for all Lucent customer products and business activities in India. Dr. Borkar develops knowledge share and teaches advanced courses in Telecommunications and Computer Architecture for the Academia, IEEE, and the industry. He has been an organizer and moderator of conferences and panel discussions on WiMAX and VoIP/Next Generation Networks (NGNs). Dr. Borkar received his B. Tech. in Electrical Engineering from Indian Institute of Technology Delhi (India) and M.S. and Ph. D. in ECE from Illinois Institute of Technology, Chicago.